

# Integrated Security for the Branch and WAN Edge

BRKSEC-2002

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Agenda

- SAFE for the Branch and WAN Edge
  - Key Areas of Threat Focus
  - Overall SAFE approach
- Threat Focus in Detail
  - Threats, mitigation tools, design and integration
- Visibility through Telemetry
  - Role, design and integration
- Threat Mitigation in Action
- Branch and WAN Edge Security Review

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Branch and WAN Edge Security Intro

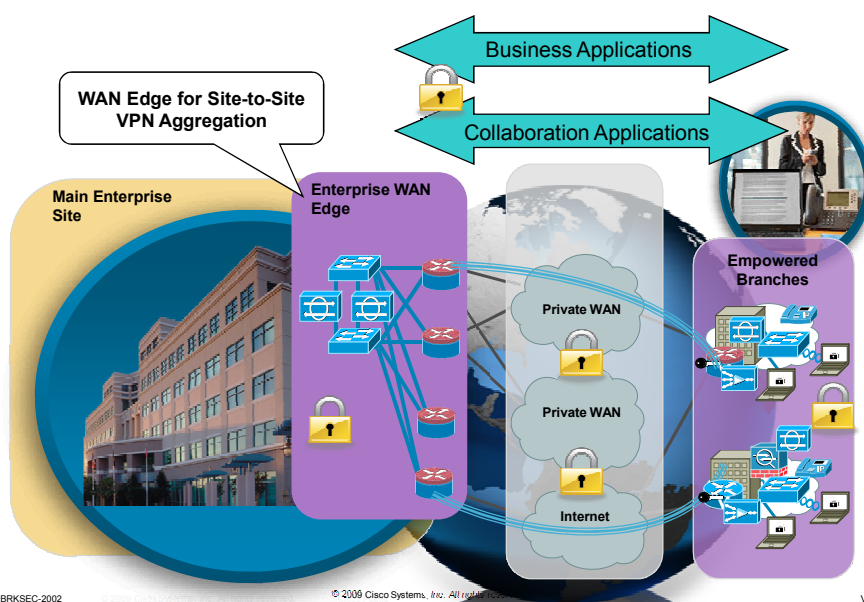
SAFE Branch and WAN Edge

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Typical Branch and WAN Edge Architecture



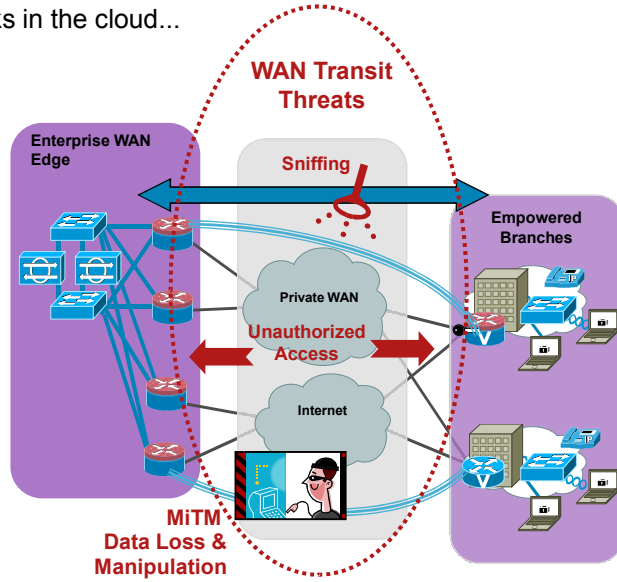
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Branch and WAN Edge: Threat Focus Area #1

Attacks in the cloud...



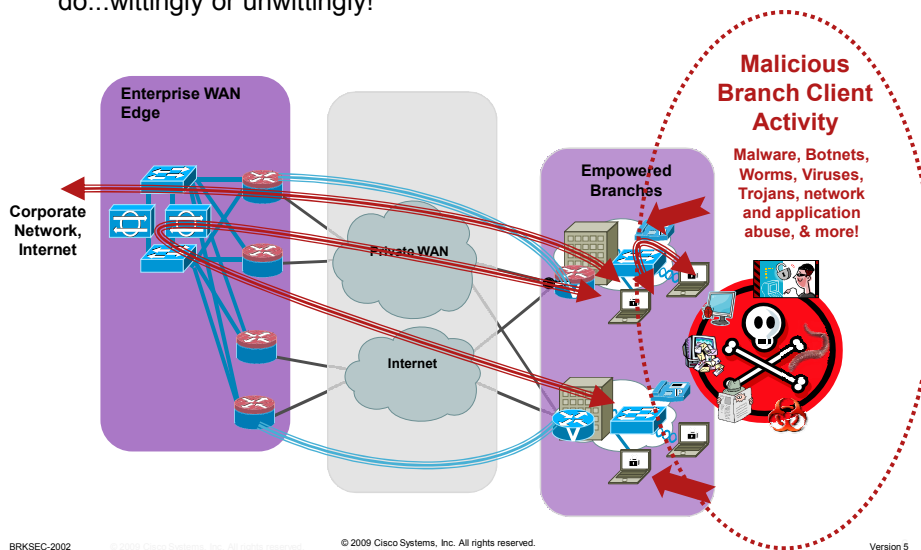
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Branch and WAN Edge: Threat Focus Area #2

All the bad things endpoints are subjected to and do...wittingly or unwittingly!

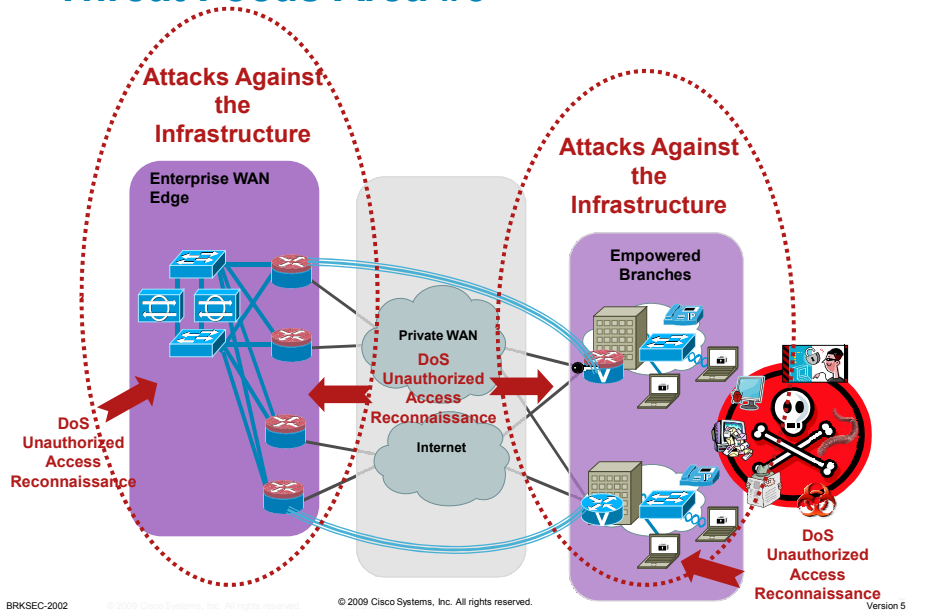


BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Branch and WAN Edge: Threat Focus Area #3



## Be Prepared: Cisco SAFE for the Branch and WAN Edge

		Threat Focus	Threats Mitigated	Security Objectives	Security Integration
Control	• Network Foundation Protection	Attacks against the infrastructure itself	Unauthorized access to devices, network and data Reconnaissance DoS	Deliver resilient and highly available network services	<ul style="list-style-type: none"> <li>• Routing Security</li> <li>• Service Resiliency</li> <li>• Network Policy Enforcement</li> <li>• Switching Security</li> <li>• Secure Device Access</li> </ul>
	• Threat Control and Containment	WAN transit threats  Malicious branch client activity	Unauthorized access to network and data E.g. Sniffing, man-in-the-middle (MITM) attacks  Malware proliferation, botnets, worms, viruses, Trojans Application and network abuse	Isolate and secure WAN data and access  Harden the endpoint Isolate and enforce security domains Detect and mitigate threats	<ul style="list-style-type: none"> <li>• Secure WAN Connectivity</li> <li>• Endpoint Security</li> <li>• Firewall Integration</li> <li>• Web Security</li> <li>• Email Security</li> <li>• IPS Integration</li> </ul>
Visibility	• Monitoring, Analysis and Correlation	Cross-network intelligence		Monitor the network Detect anomalies Correlate threats	<ul style="list-style-type: none"> <li>• SNMP, Syslog, SDEE, AAA, Netflow</li> <li>• CS-MARS</li> <li>• Cross-platform collaboration</li> <li>• Global correlation</li> </ul>

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



# Threat Focus Area #1: WAN Transit Threats

SAFE Branch and WAN Edge

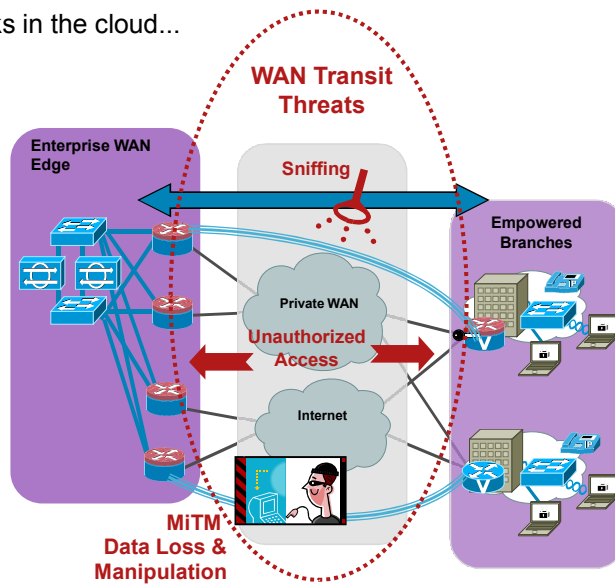
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## WAN Transit Threats

Attacks in the cloud...



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Secure WAN Connectivity: Site-Site VPN Security Principles



- Isolate WAN Traffic

Segment corporate WAN traffic from other traffic on the WAN to enable the confidentiality and integrity of data

Dedicated point-to-point link, corporate managed VPN, Service Provider managed MPLS service, etc.



- Authenticate WAN Access

Access to the corporate WAN must feature a strong authentication mechanism to prevent unauthorized access to the network and data

Public Key Infrastructure (PKI) for strong tunnel authentication and scalable, manageable deployment

Pre-shared key (PSK) as an alternative



- Encrypt WAN Traffic

Data in transit over the WAN may need to be encrypted if the WAN is vulnerable to data loss and manipulation, sensitive data is being transmitted or for compliance reasons

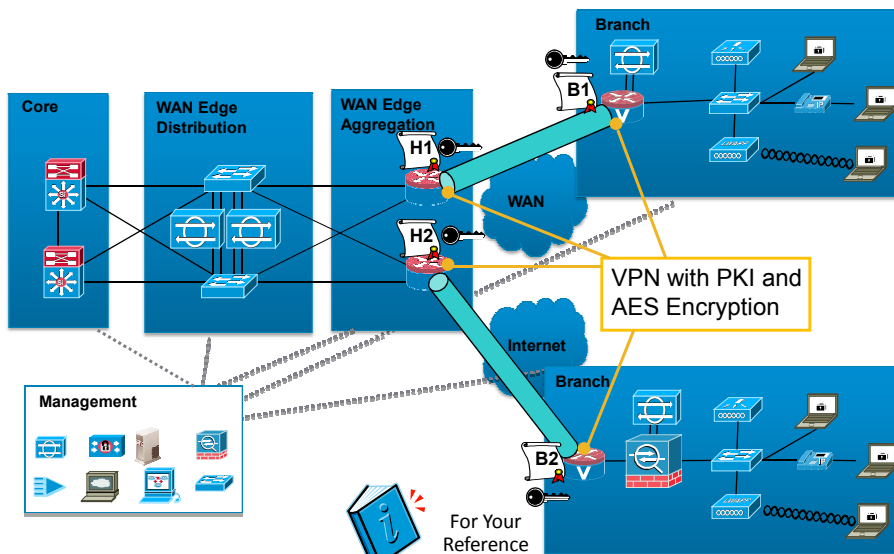
Advanced Encryption Standard (AES) for strong encryption

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Secure Site-to-Site VPN



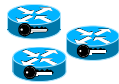
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

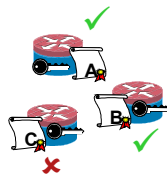
## VPN Tunnel Authentication: PSK vs PKI

- Pre-shared key (PSK)



- Easy to deploy but manageability challenges
- Security dependent on the strength of the pre-defined keys
- Keys tied to unique IP address
  - Wild card pre-shared keys required for dynamically assigned IP address spokes
  - => If wild card key compromised, ALL spokes must be provisioned with a new key

- Public Key Infrastructure (PKI)



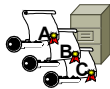
- Certificate-based, scalable and manageable strong authentication that is critical to large-scale VPN deployments
- Requires initial investment but enables dynamic renewal and revocation of certificates
  - => Dynamic commissioning and decommissioning of branches with ease
- Don't forget to secure the PKI itself!

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Securing the PKI Itself



- Extend network foundation protection security principles to the PKI:

- Certificate Database

- Hardened host with minimum, highly controlled access, typically in restricted area of data center.

- CRL/CDP Server

- Hardened host with minimum, controlled access.



- Use non-standard port to obfuscate + enforce firewall and ACL policies to only permit this traffic.

- CA servers – Hierarchical Model

- Root-CA on hardened device with minimum, controlled access, typically in restricted area of data center. Often offline unless required.



- Sub-CAs on hardened devices with minimum, controlled access. Location dependent on enrollment and re-enrollment policy, external behind a firewall if automated enrollment deployed.

- Do not automatically grant certificates!



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample PKI Config for VPN Hub

- Enrollment to sub-CA on non-standard port
- CRL checking performed to verify validity of spoke certificates
- Auto-enrollment at 70% of certificate validity period

```
crypto pki trustpoint <subCA-1>  
enrollment url http://<subCA-1>:12345
```

```
revocation-check crl  
auto-enroll 70 regenerate
```

```
storage bootflash:
```

```
!
```

- If CRL not reliably available, can fall back to no CRL if not available
  - Lower TCP timeout to minimize fall back time
- ```
revocation check crl none  
ip tcp synwait-time 5
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Threat Focus Area #2: Malicious Branch Client Activity

SAFE Branch and WAN Edge

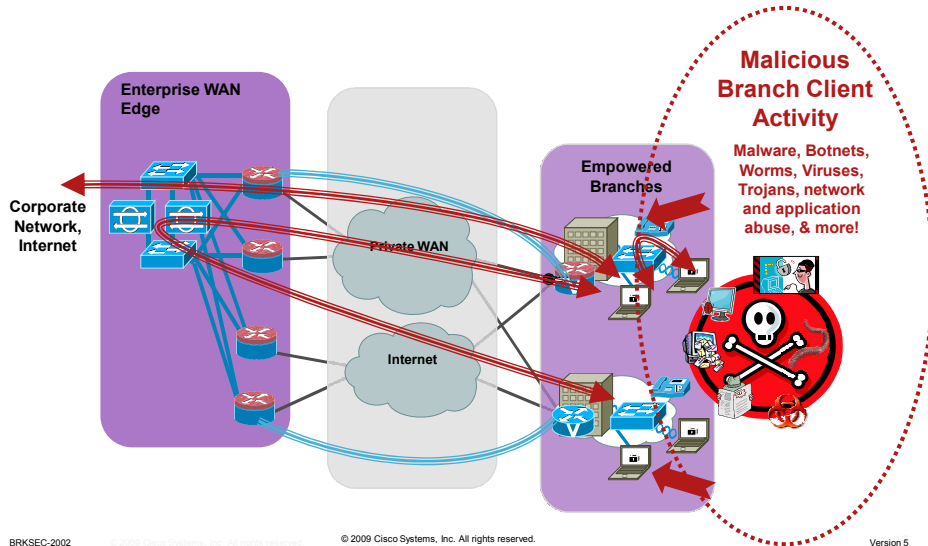
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Malicious Branch Client Activity

When the bad guys are on the inside...



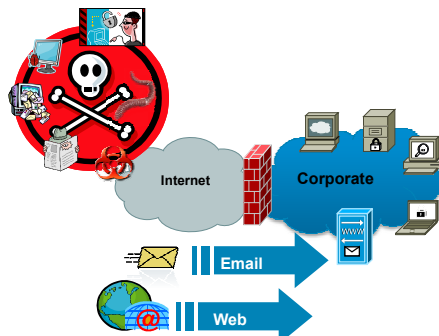
## Bad Guys on the Inside?

- But you control the perimeter & don't let the bad guys on the inside

Trusted users only on the inside



- Do you permit these business applications?



# Malware Embedded in Incoming Email

- Spam, phishing, virus and malware in legitimate incoming email



Solutions Products & Services Ordering Support Training & Events Partner Central

Security Center

### Threat Outbreak Alerts

Threat Outbreak Alerts cover the latest data regarding malicious email-based and web-based threats, including spam, phishing, viruses, malware, and botnet activity.

| Title                                                                                                                                                  | Date           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|
| <a href="#">Threat Outbreak Alert: Misleading Photo E-Mail Messages on May 3, 2009</a> <b>New!</b>                                                     | May 06, 2009   |
| <a href="#">Threat Outbreak Alert: Fake E-Mail Messages With Petrobras Information on May 5, 2009</a> <b>New!</b>                                      | May 06, 2009   |
| <a href="#">Threat Outbreak Alert: Fake Police Raid on Nightclub E-Mail Messages on May 5, 2009</a> <b>New!</b>                                        | May 05, 2009   |
| <a href="#">Threat Outbreak Alert: Misleading Brazilian Internet Banking Company Security Update E-Mail Messages on April 30, 2009</a> <b>Updated!</b> | April 30, 2009 |
| <a href="#">Threat Outbreak Alert: Fake Macromedia Flash Version Upgrade E-Mail Messages on April 30, 2009</a> <b>New!</b>                             | April 30, 2009 |
| <a href="#">Threat Outbreak Alert: Fake Image File Sharing E-Mail Messages on April 30, 2009</a> <b>New!</b>                                           | April 30, 2009 |
| <a href="#">Threat Outbreak Alert: Misleading Banco Rau Security Update E-Mail Messages on April 6, 2009</a> <b>Updated!</b>                           | April 27, 2009 |
| <a href="#">Threat Outbreak Alert: Work/Pay Card False Credit Transaction E-Mail Messages on April 24, 2009</a>                                        | April 24, 2009 |
| <a href="#">Threat Outbreak Alert: Adult Video E-mail Messages on April 21, 2009</a> <b>New!</b>                                                       | April 21, 2009 |
| <a href="#">Threat Outbreak Alert: Fake Hallmark E-Card Messages with Executable File Attachment on April 20, 2009</a> <b>New!</b>                     | April 20, 2009 |

Showing 1-10 of 111 | 1 | Next >

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Malware Embedded in Web Sites

- Malicious web sites
- Malware embedded in compromised legitimate web sites
- Links to malware downloads on legitimate sites



\*\*\* More info in BRKSEC-2052 - Hacked While Browsing. Using the Web to Spread Malware \*\*\*

According to security audit provider White Hat Security >79% of sites hosting malicious code are legitimate websites.

### Part of This Website is Compromised



Home > News > BusinessWeek website compromised

### BusinessWeek website compromised

Chuck Miller September 16, 2008

PRINT EMAIL REPRINT PERMISSIONS FOR

The BusinessWeek magazine website has been infected that could redirect visitors to malicious servers

### New worms target both MySpace and Facebook users

Kaspersky Lab, a leading developer of secure content management systems, has announced the discovery of two new variants of a new worm, Net-Worm.Win32.Koobface.a, and Net-Worm.Win32.Koobface.b, which are designed to attack MySpace and Facebook respectively. As part of their malicious payload, the worms transform victim machines into zombie computers to form botnets.

Even though the worms are currently only infecting MySpace and Facebook users, analysts are warning users that the worms are designed to upload additional malware with other functionality via the Internet. It is highly probable that victim machines will be used for spreading links via these social networking sites, but the botnets will also be used for malicious purposes.

### Kaspersky and Bitdefender Websites Hacked

The databases were compromised through SQL injection attacks



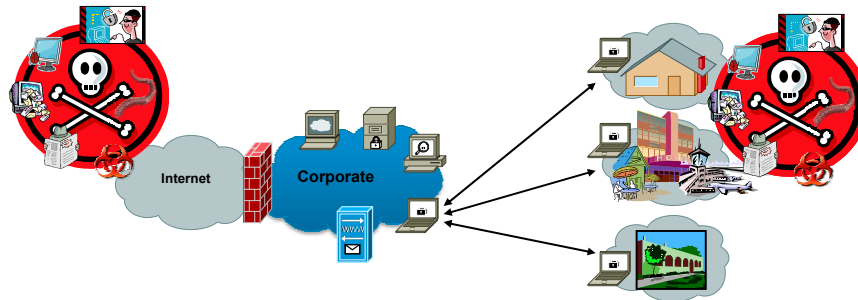
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Bad Guys on the Inside?

- Do you have mobile clients?
- Do your mobile clients connect to other networks?
- Are those networks highly secure?
- Do those mobile clients come back into your network?



BRKSEC-2002

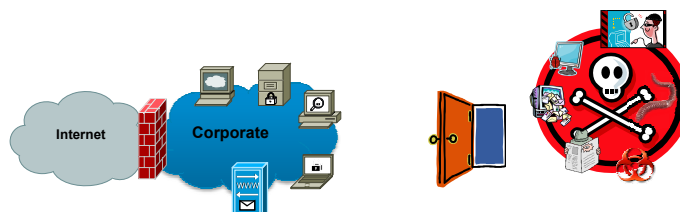
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Bad Guys on the Inside?



- Do you have strong physical security for access to the building?
- Do you have strong physical security for access to your networking gear?
- Do guests, vendors, partners, contractors, etc. access your network?
- Do you control all machines on the network?



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Local Malware



- Malware on local connections, local host

LAN, Internet, WLAN, Bluetooth, removable media, network shares, etc.

Worms, viruses, Trojans, botnets, buffer overflows, resource exhaustion attacks, spyware, rootkits, application vulnerabilities, unauthorized access, theft of information, data leakage etc.

### Conficker (AKA Downadup or Kido) Infections Skyrocket To An Estimate 9 Million

Darknet spilled these bits on January 19th 2009 @ 4:24 pm

There hasn't been a viral outbreak of this scale for quite some time, Conficker or Downadup as it's known was only fairly recently discovered (Oct 2008) and has already infected an estimated 9 million machines!

It's spreading fast though and it auto-updates itself via downloads from random domains making it almost impossible to stop as whatever countermeasures come out, it can just download itself the latest version and bypass them.

It also has multiple infection vectors including travelling via USB drives.



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Common Endpoint Attack Vectors



- Email

Malware embedded in incoming emails

Phishing



- Web

Malware embedded in legitimate web sites

Malware embedded in requested downloads

Malware embedded in malicious sites



- Local connectivity

Malware propagation through the LAN, WLAN, Bluetooth, removable media, network shares, etc.

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## Target: Endpoint



- Goal here is to own the endpoint  
Client, server, handset, etc.
- Once you own the endpoint, you have access to:
  - Locally stored data, confidential company information, personal data
  - Conversations – usernames/passwords, bank a/c, credit card transactions, host access credentials, etc.
  - Access to trusted resources of the host machine/user
  - Other hosts for further propagation
- Plus, you have a launch pad for attacks  
DoS, spam, fraud, theft of information

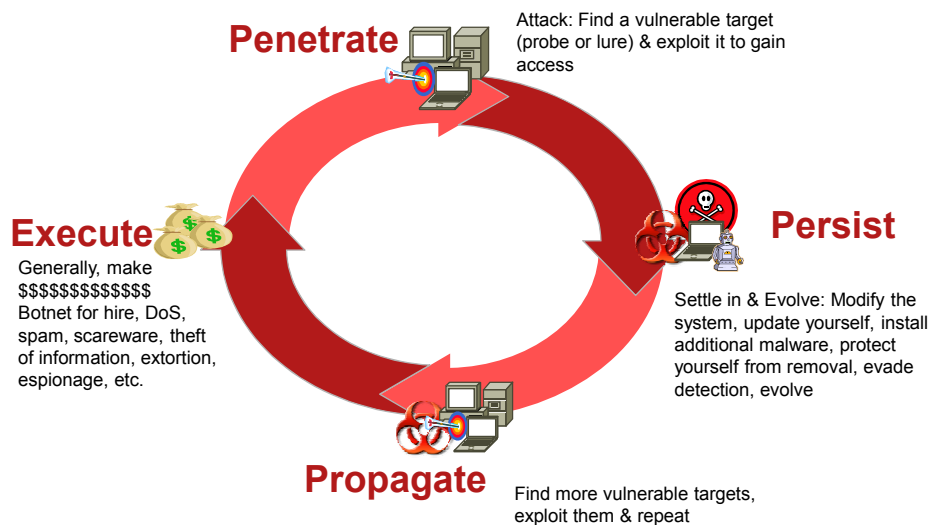
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Threat Detection and Mitigation

*Malware has a general pattern...*











BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Today's Malware Follow the Same Pattern...

Recent example, Gumblar

- ▪ Leverages proliferation of web sites without adequate security  
Compromises legitimate sites....redirects to malicious
- ▪ Leverages widespread JavaScript enablement in clients to deliver malware
- ▪ Leverages latest vulnerabilities to exploit clients  
Users not yet patched (Adobe PDF & Flash Player)
- ▪ Employs evasion and self-protection techniques to avoid detection and removal  
Disables security software, installs fake anti-virus
- ▪ Installs a sniffer to steal FTP credentials & installs a backdoor to maintain server access  
Provides further sites to compromise, creating a botnet of infected web sites for widest impact and ongoing malware delivery
- ▪ Hijacks Google search queries to redirect to further sites hosting malware
- ▪ Morphs to enable persistence  
Continually updates itself with new malware, new command & control information, new domain information, dynamically generated and obfuscated JavaScript
- ▪ Classic money generator - installs a spam bot (someone has to pay the bills!)



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Mitigating Remote Endpoint Threats

*Same principles as across the corporate network...*

- ▪ Mitigate the initial infection
  - Email security
  - Web security
  - Endpoint security
- ▪ Detect & mitigate malicious behavior
  - IPS integration
  - Firewall integration
  - Traffic monitoring

*....mitigate as close to the source as possible*

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Mitigate the Initial Infection: Malware in Email

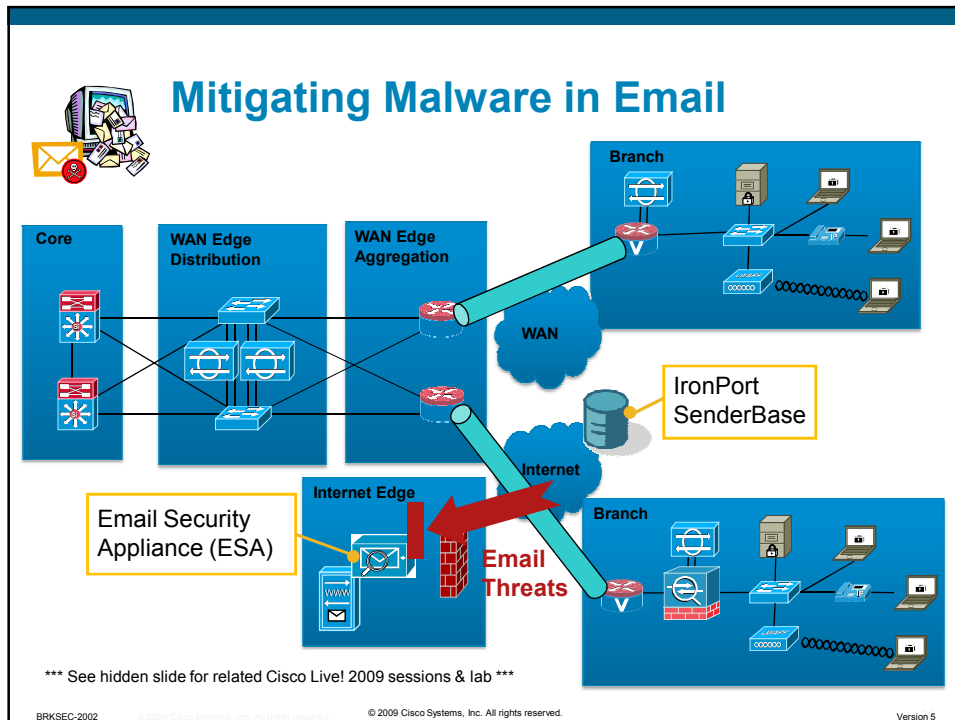
SAFE Branch and WAN Edge



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## Email Security



- Email-based threat mitigation

C-Series Email Security Appliance (ESA) in collaboration with IronPort SenderBase

Reputation-based filtering - Blocks 80% of spam

Content-based filtering (Anti-Spam)

More detailed analysis for anomalies in content

Virus outbreak filters from ironport.com

Timely virus blocking , prior to software patch & AV update availability and deployment

Also offers Data Loss Prevention policies and email encryption for outgoing email



Related Cisco Live! 2009 sessions:

- BRKSEC-2001 - Security Considerations and Design Framework for the Internet Edge Enterprise Network
- BRKSEC-2546 - Preventing Spam, Viruses, and Data Loss with IronPort Email Security Appliances
- LTRSEC-2546 - IronPort Email Security Technology Overview



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Mitigate the Initial Infection: Malware in External Web Sites

SAFE Branch and WAN Edge



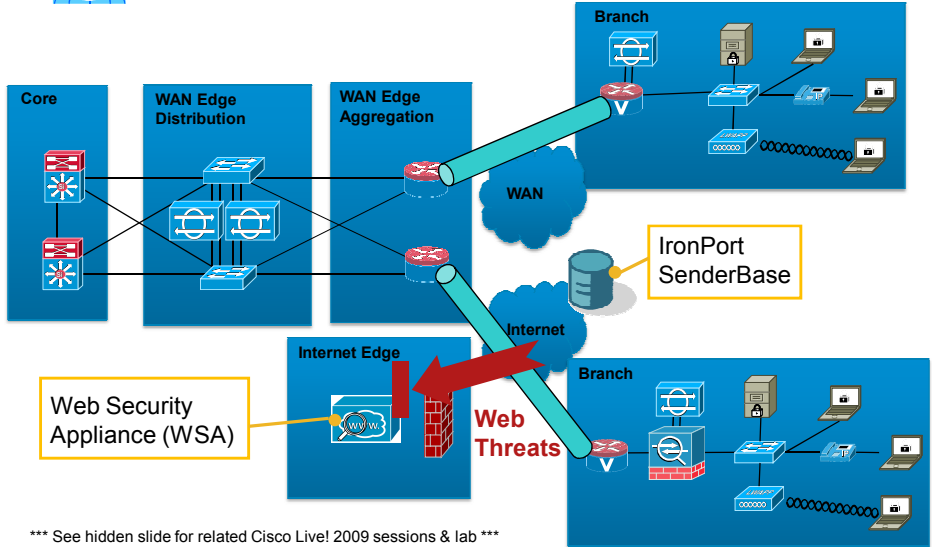
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



# Mitigating Malware in External Web Sites: Centralized Internet Access



\*\*\* See hidden slide for related Cisco Live! 2009 sessions & lab \*\*\*

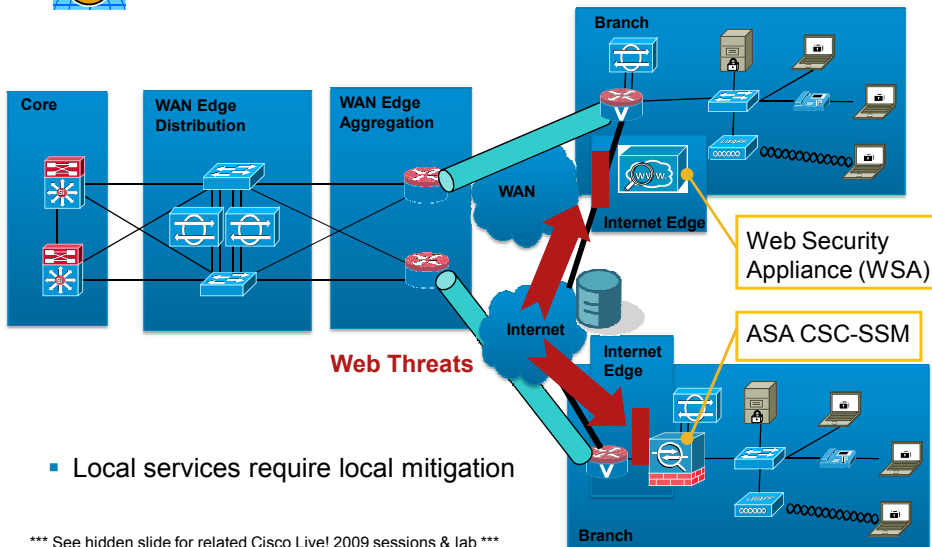
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



# Mitigating Malware in External Web Sites: Local Internet Access



- Local services require local mitigation

\*\*\* See hidden slide for related Cisco Live! 2009 sessions & lab \*\*\*

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## External Web Security

- Web-based threat mitigation



Web Security Appliance (WSA) in collaboration with IronPort SenderBase

Layer 4 Traffic Monitor

Detects anomalous traffic across all ports

Reputation-based filtering

URI-based behavior and attribute analysis - Blocks 70% of known & unknown malware traffic at connection time

Content-based filtering (DVS)

More detailed analysis for anomalies in content

Also offers Acceptable Use Policy enforcement and Data Loss Prevention features



Related Cisco Live! 2009 sessions:

- BRKSEC-2001 - Security Considerations and Design Framework for the Internet Edge Enterprise Network
- BRKSEC-2545 - Introduction to IronPort Web Security
- LTRSEC-2545 - IronPort Web Security Technology Overview



For Your Reference

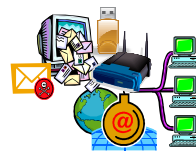
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Mitigate the Initial Infection: Direct Endpoint Compromise

SAFE Branch and WAN Edge



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Mitigating Direct Endpoint Compromise: Endpoint Security Principles

*If you manage the endpoint, prepare it for the big bad world...*



- Protect against known attacks

Signature-based threat detection and mitigation, such as known worms and viruses.



- Protect against zero-day or unpatched attacks

Behavioral-based threat detection and mitigation, such as new exploits and new malware.



- Enforce policy

Visibility into and protection against non-compliant behavior such as data loss, unauthorized access, network and application abuse.

*....protect the endpoint, whichever network they may be on, whoever they may trust*

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## CSA Endpoint Security: Host-Based IPS

- Endpoint protection in every location, every threat vector

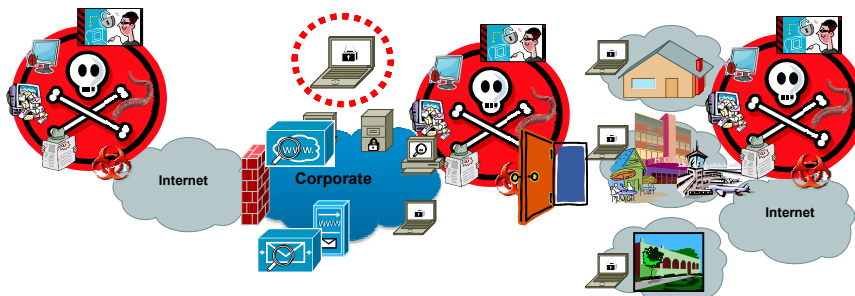
Known threats

Unknown threats

All threat vectors: network, web, email, local media, etc.

- Policy enforcement

Network and application abuse, acceptable use, DLP



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# CSA: Behavioral-Based Host IPS

*"That's not normal..."*

- CSA behavioral-based threat detection & mitigation

| Malware Behaviors                     |
|---------------------------------------|
| Access or Modify System Configuration |
| Buffer overflow                       |
| Invoking Command Shell or Config Apps |
| Modify another process                |
| Monitor User Input                    |
| Network Protocols                     |
| Network Worm Client                   |

- Monitors system calls for malware behavior
  - File system, Registry, Network, Execution space
- Verifies application calls for system resources

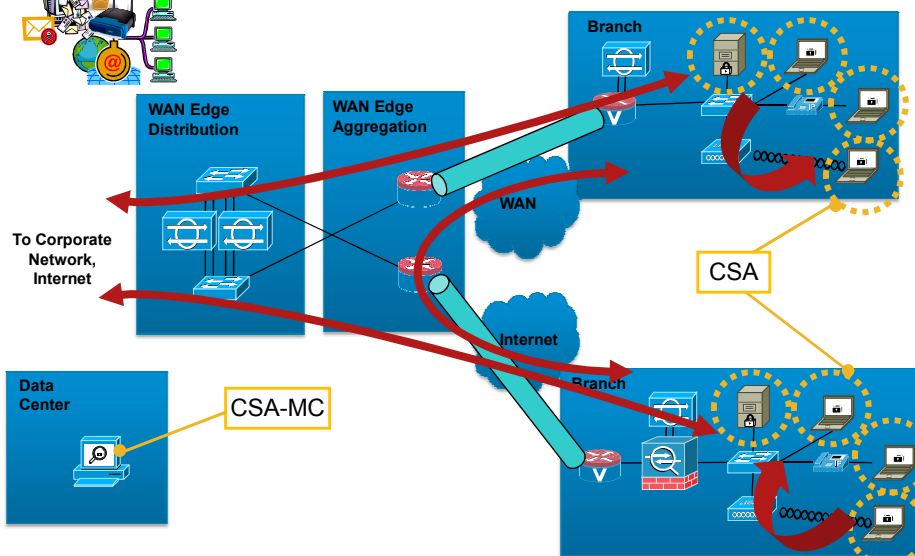


BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Mitigating Direct Endpoint Compromise



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## CSA for Remote Endpoints



- Centralized CSA-MC

Leverage common, consistent policies across all endpoints



- WAN outage is not an issue

CSA continues to protect the endpoint even if corporate connectivity is lost

- Beware of policies based on CSA-MC reachability

CSA offers location-aware policies, including CSA-MC reachability, such as for VPN enforcement. Think them through before you enforce them!

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Don't forget the ultimate endpoint – the user!



- User education and training

User behavior is a key factor in endpoint and overall network security

Becoming even more critical as attacks evolve to focus on social engineering and targeted attacks

CSA can be leveraged to reinforce user education and training, and monitor user behavior



For instance, advising users when they perform an anomalous action, the risks it presents and the associated corporate policy

A default action can be enforced or the user can be allowed to decide

A justification can be required to provide an audit trail

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Detect & Mitigate Malicious Behaviour: IPS Integration

SAFE Branch and WAN Edge



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Threat Detection & Mitigation with Network IPS

- Monitor network traffic to detect and mitigate anomalous behavior

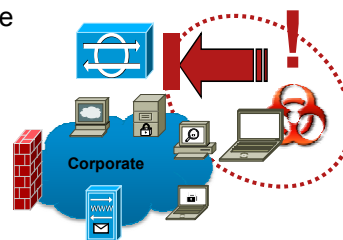
Attacks against your internal web servers

Viruses, Worms, Trojans

Botnets

Attacks against your infrastructure

Covert channeling



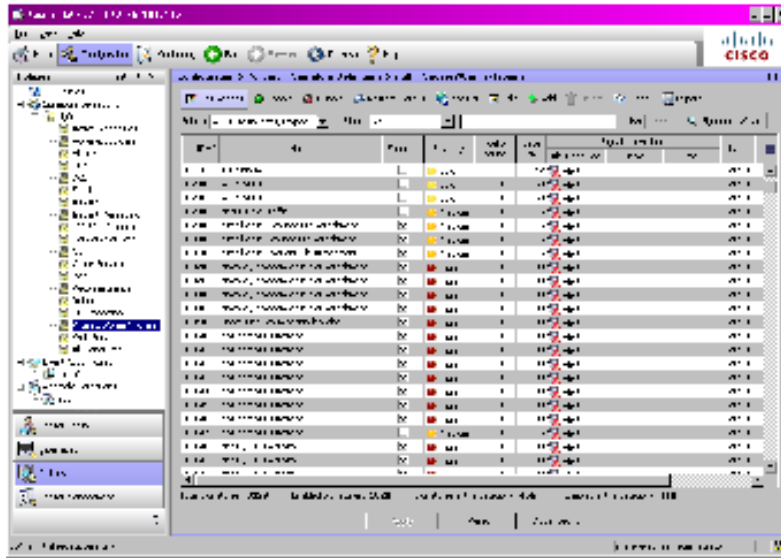
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



# Viruses, Worms, Trojans

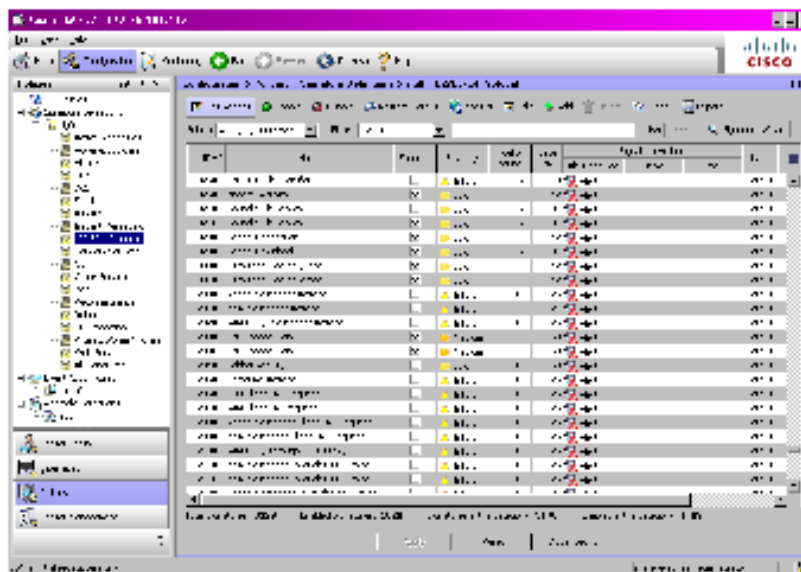


BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Botnets



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Attacks Against UC

| First Name | Last Name | Phone Number | Status | Account Type | Account ID | Account ID | Account ID | Account ID | Account ID |
|------------|-----------|--------------|--------|--------------|------------|------------|------------|------------|------------|
| John       | Doe       | 3105551234   | Active | Standard     | 1000000000 | 1000000000 | 1000000000 | 1000000000 | 1000000000 |
| Jane       | Smith     | 3105555678   | Active | Standard     | 1000000001 | 1000000001 | 1000000001 | 1000000001 | 1000000001 |
| Bob        | Johnson   | 3105559012   | Active | Standard     | 1000000002 | 1000000002 | 1000000002 | 1000000002 | 1000000002 |
| Alice      | Williams  | 3105553456   | Active | Standard     | 1000000003 | 1000000003 | 1000000003 | 1000000003 | 1000000003 |
| Charlie    | Brown     | 3105557890   | Active | Standard     | 1000000004 | 1000000004 | 1000000004 | 1000000004 | 1000000004 |
| Diana      | Green     | 3105552345   | Active | Standard     | 1000000005 | 1000000005 | 1000000005 | 1000000005 | 1000000005 |
| Frank      | White     | 3105556789   | Active | Standard     | 1000000006 | 1000000006 | 1000000006 | 1000000006 | 1000000006 |
| Grace      | Black     | 3105550123   | Active | Standard     | 1000000007 | 1000000007 | 1000000007 | 1000000007 | 1000000007 |
| Henry      | Grey      | 3105554567   | Active | Standard     | 1000000008 | 1000000008 | 1000000008 | 1000000008 | 1000000008 |
| Ivy        | Blue      | 3105558901   | Active | Standard     | 1000000009 | 1000000009 | 1000000009 | 1000000009 | 1000000009 |
| Jack       | Gold      | 3105552345   | Active | Standard     | 1000000010 | 1000000010 | 1000000010 | 1000000010 | 1000000010 |
| Karen      | Silver    | 3105556789   | Active | Standard     | 1000000011 | 1000000011 | 1000000011 | 1000000011 | 1000000011 |
| Leo        | Platinum  | 3105550123   | Active | Standard     | 1000000012 | 1000000012 | 1000000012 | 1000000012 | 1000000012 |
| Mia        | Palladium | 3105554567   | Active | Standard     | 1000000013 | 1000000013 | 1000000013 | 1000000013 | 1000000013 |
| Noah       | Gold      | 3105558901   | Active | Standard     | 1000000014 | 1000000014 | 1000000014 | 1000000014 | 1000000014 |
| Olivia     | Silver    | 3105552345   | Active | Standard     | 1000000015 | 1000000015 | 1000000015 | 1000000015 | 1000000015 |
| Peter      | Platinum  | 3105556789   | Active | Standard     | 1000000016 | 1000000016 | 1000000016 | 1000000016 | 1000000016 |
| Quinn      | Palladium | 3105550123   | Active | Standard     | 1000000017 | 1000000017 | 1000000017 | 1000000017 | 1000000017 |
| Rachel     | Gold      | 3105554567   | Active | Standard     | 1000000018 | 1000000018 | 1000000018 | 1000000018 | 1000000018 |
| Samuel     | Silver    | 3105558901   | Active | Standard     | 1000000019 | 1000000019 | 1000000019 | 1000000019 | 1000000019 |
| Tina       | Platinum  | 3105552345   | Active | Standard     | 1000000020 | 1000000020 | 1000000020 | 1000000020 | 1000000020 |
| Uma        | Palladium | 3105556789   | Active | Standard     | 1000000021 | 1000000021 | 1000000021 | 1000000021 | 1000000021 |
| Victor     | Gold      | 3105550123   | Active | Standard     | 1000000022 | 1000000022 | 1000000022 | 1000000022 | 1000000022 |
| Wendy      | Silver    | 3105554567   | Active | Standard     | 1000000023 | 1000000023 | 1000000023 | 1000000023 | 1000000023 |
| Xavier     | Platinum  | 3105558901   | Active | Standard     | 1000000024 | 1000000024 | 1000000024 | 1000000024 | 1000000024 |
| Yara       | Palladium | 3105552345   | Active | Standard     | 1000000025 | 1000000025 | 1000000025 | 1000000025 | 1000000025 |
| Zoe        | Gold      | 3105556789   | Active | Standard     | 1000000026 | 1000000026 | 1000000026 | 1000000026 | 1000000026 |

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Attacks Against DNS

| First Name | Last Name | Phone Number | Status | Account Type | Account ID | Account ID | Account ID | Account ID | Account ID |
|------------|-----------|--------------|--------|--------------|------------|------------|------------|------------|------------|
| John       | Doe       | 3105551234   | Active | Standard     | 1000000000 | 1000000000 | 1000000000 | 1000000000 | 1000000000 |
| Jane       | Smith     | 3105555678   | Active | Standard     | 1000000001 | 1000000001 | 1000000001 | 1000000001 | 1000000001 |
| Bob        | Johnson   | 3105559012   | Active | Standard     | 1000000002 | 1000000002 | 1000000002 | 1000000002 | 1000000002 |
| Alice      | Williams  | 3105553456   | Active | Standard     | 1000000003 | 1000000003 | 1000000003 | 1000000003 | 1000000003 |
| Charlie    | Brown     | 3105557890   | Active | Standard     | 1000000004 | 1000000004 | 1000000004 | 1000000004 | 1000000004 |
| Diana      | Green     | 3105552345   | Active | Standard     | 1000000005 | 1000000005 | 1000000005 | 1000000005 | 1000000005 |
| Frank      | White     | 3105556789   | Active | Standard     | 1000000006 | 1000000006 | 1000000006 | 1000000006 | 1000000006 |
| Grace      | Black     | 3105550123   | Active | Standard     | 1000000007 | 1000000007 | 1000000007 | 1000000007 | 1000000007 |
| Henry      | Grey      | 3105554567   | Active | Standard     | 1000000008 | 1000000008 | 1000000008 | 1000000008 | 1000000008 |
| Ivy        | Blue      | 3105558901   | Active | Standard     | 1000000009 | 1000000009 | 1000000009 | 1000000009 | 1000000009 |
| Jack       | Gold      | 3105552345   | Active | Standard     | 1000000010 | 1000000010 | 1000000010 | 1000000010 | 1000000010 |
| Karen      | Silver    | 3105556789   | Active | Standard     | 1000000011 | 1000000011 | 1000000011 | 1000000011 | 1000000011 |
| Leo        | Platinum  | 3105550123   | Active | Standard     | 1000000012 | 1000000012 | 1000000012 | 1000000012 | 1000000012 |
| Mia        | Palladium | 3105554567   | Active | Standard     | 1000000013 | 1000000013 | 1000000013 | 1000000013 | 1000000013 |
| Noah       | Gold      | 3105558901   | Active | Standard     | 1000000014 | 1000000014 | 1000000014 | 1000000014 | 1000000014 |
| Olivia     | Silver    | 3105552345   | Active | Standard     | 1000000015 | 1000000015 | 1000000015 | 1000000015 | 1000000015 |
| Peter      | Platinum  | 3105556789   | Active | Standard     | 1000000016 | 1000000016 | 1000000016 | 1000000016 | 1000000016 |
| Quinn      | Palladium | 3105550123   | Active | Standard     | 1000000017 | 1000000017 | 1000000017 | 1000000017 | 1000000017 |
| Rachel     | Gold      | 3105554567   | Active | Standard     | 1000000018 | 1000000018 | 1000000018 | 1000000018 | 1000000018 |
| Samuel     | Silver    | 3105558901   | Active | Standard     | 1000000019 | 1000000019 | 1000000019 | 1000000019 | 1000000019 |
| Tina       | Platinum  | 3105552345   | Active | Standard     | 1000000020 | 1000000020 | 1000000020 | 1000000020 | 1000000020 |
| Uma        | Palladium | 3105556789   | Active | Standard     | 1000000021 | 1000000021 | 1000000021 | 1000000021 | 1000000021 |
| Victor     | Gold      | 3105550123   | Active | Standard     | 1000000022 | 1000000022 | 1000000022 | 1000000022 | 1000000022 |
| Wendy      | Silver    | 3105554567   | Active | Standard     | 1000000023 | 1000000023 | 1000000023 | 1000000023 | 1000000023 |
| Xavier     | Platinum  | 3105558901   | Active | Standard     | 1000000024 | 1000000024 | 1000000024 | 1000000024 | 1000000024 |
| Yara       | Palladium | 3105552345   | Active | Standard     | 1000000025 | 1000000025 | 1000000025 | 1000000025 | 1000000025 |
| Zoe        | Gold      | 3105556789   | Active | Standard     | 1000000026 | 1000000026 | 1000000026 | 1000000026 | 1000000026 |

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## P2P Application Use

| IP         | To         | From       | Prio | App        | Bytes   |
|------------|------------|------------|------|------------|---------|
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1000000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 500000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 750000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1200000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 600000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 800000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1100000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 550000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 700000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1300000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 650000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 850000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1400000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 700000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 900000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1500000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 750000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 950000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | BitTorrent | 1600000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | eMule      | 800000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | uTorrent   | 1000000 |

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Anomalous Activity

| IP         | To         | From       | Prio | App    | Bytes   |
|------------|------------|------------|------|--------|---------|
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1000000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 500000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 750000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1200000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 600000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 800000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1100000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 550000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 700000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1300000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 650000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 850000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1400000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 700000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 900000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1500000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 750000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 950000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | HTTP   | 1600000 |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | FTP    | 800000  |
| 10.10.10.1 | 10.10.10.2 | 10.10.10.1 | 1    | Telnet | 1000000 |

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

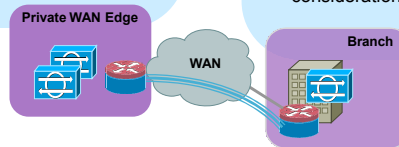
## Deployment Models for Branch IPS Integration

### Centralized IPS

- Cost-effective, highly scalable, highly available
- Highly effective in a hub-and-spoke topology where all branch traffic is forced through the central site
- Coverage limited to traffic passing through WAN edge
  - Intra-branch traffic not analyzed
  - Branch-branch traffic requires traffic to be forced through IPS

### Distributed IPS

- Highly effective, localized threat detection and mitigation
  - Mitigation as close to source as possible to minimize potential impact on rest of network
- Often required for certain deployments
  - Local, direct Internet access through the use of split-tunneling
  - Spoke-spoke deployment models
  - PCI compliance
- Cost and manageability considerations



Deployments often leverage a mix of both, according to the profile of the branch

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Cisco IPS Platform Choices

- Wide range of IPS platforms that can be selected according to the deployment model and particular site needs

### IOS IPS



- Cost-effective, integrated, software-based IPS
- Sub-set of signatures
- No collaboration with WLAN controller or SensorBase

### IPS Series



- Highly scalable, high availability, hardware-based IPS
- Common, rich signature set
- Collaboration with SensorBase for global correlation, WLAN controller\*
- Facilitates separate administrative domains (NetOps vs SecOps)
- Dedicated appliances and integrated modules for ISR, ASA and Cat6k

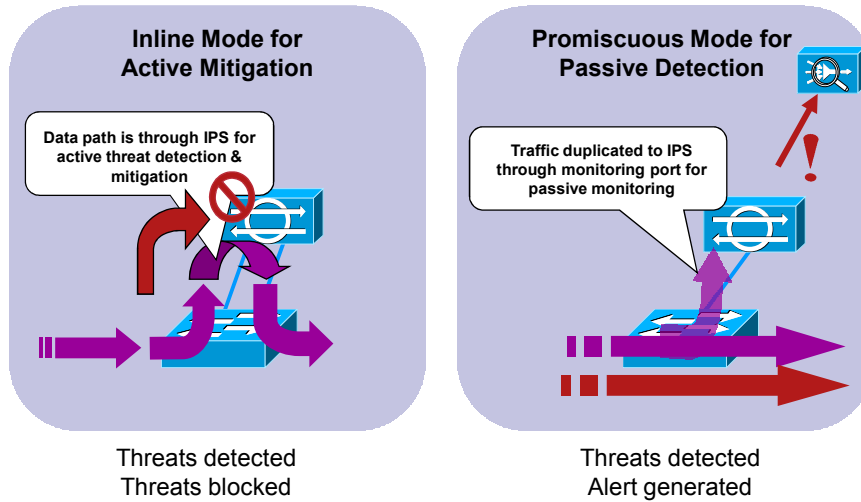
\* Global correlation is not currently available on an IPS module in an ASA 5505

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Cisco IPS Deployment Modes



BRKSEC-2002

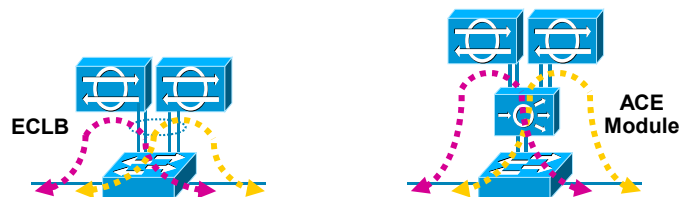
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Designing for IPS High Scalability & Availability

- For increased scalability and high availability, multiple IPS can be deployed using an intelligent load-balanced design

E.g. a dedicated load-balancing appliance, such as the ACE module, the ether channel load-balancing (ECLB), CEF load balancing, policy-based routing (PBR).



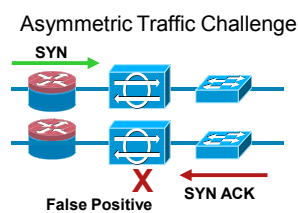
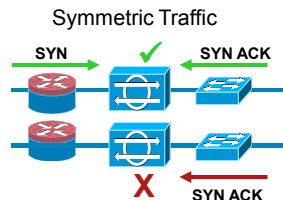
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## IPS and Symmetrical Traffic Flows



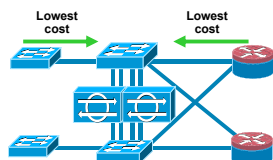
- IPS are stateful devices
  - Rely on seeing symmetrical flows to accurately detect anomalies
  - Traffic symmetry becomes a design consideration once more than one IPS in the traffic path
- Symmetrical Flow Benefits
  - Enhanced threat detection
  - Reduced false positives
  - Reduced false negatives
  - Reduced vulnerability to IPS evasion techniques

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## IPS and Symmetrical Flow Options



- Single IPS Switch
  - Dedicated IPS switch + ECLB on the switch
  - Introduces single point of failure
- Routing Manipulation
  - Routing path cost manipulation to force traffic through preferred switch
  - May be a challenge with NetOps
- Sticky Load-Balancing
  - Introducing an ACE module avoids any routing changes
  - Most expensive solution

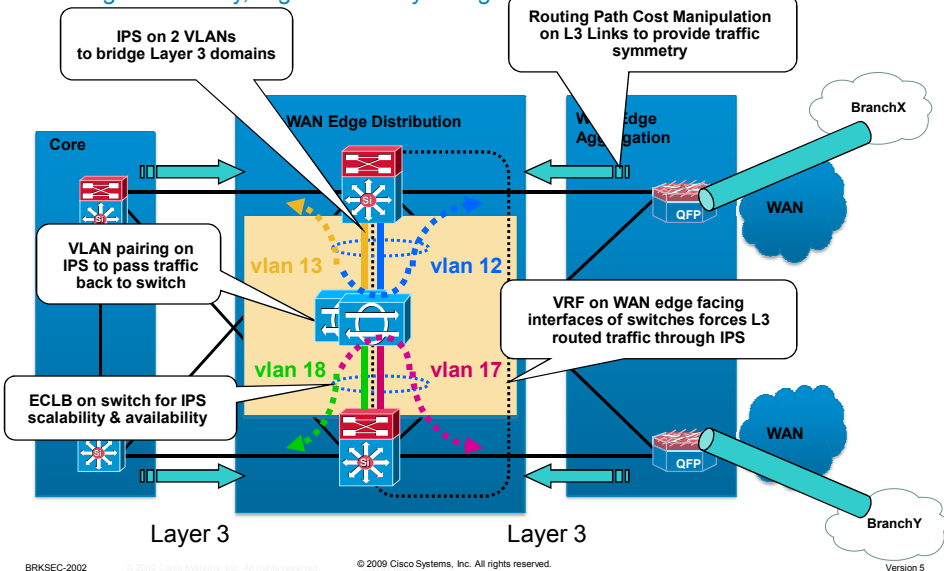
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Sample Centralized IPS Design Using Routing Manipulation

High Scalability, High Availability Design



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Sample Centralized IPS Design Using Routing Manipulation

## • Edge Router Dual Paths to Switch:

```
interface GigabitEthernet0/0/1
description To switch-1
ip address 10.208.10.2 255.255.255.252
```

```
interface GigabitEthernet0/0/2
description To switch-2
ip address 10.208.16.2 255.255.255.252
```

## • Edge Router Routing Path Cost Manipulation:

```
router eigrp 1
offset-list 0 out 50 GigabitEthernet0/0/2
```

## • Switch-1 VRF to Segment Path to Edge Router:

```
ip vrf BRANCHES
description VRF for IPS Monitoring of Branch Traffic
rd 11:1
route-target export 12:1
route-target import 12:1
```

```
router eigrp 1
address-family ipv4 vrf BRANCHES
network 10.0.0.0
no auto-summary
autonomous-system 1
exit-address-family
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Centralized IPS Design Using Routing Manipulation

### Switch-1 VLAN Pairs for IPS Integration

```
interface Vlan12
description IPS From Branches
ip vrf forwarding branches
ip address 10.208.12.1 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 eigrp-auth
load-interval 60
!
interface Vlan13
description IPS To Branches
ip address 10.208.12.2 255.255.255.252
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 eigrp-auth
load-interval 60
```

Note1: The VLANs are different but the subnet is the same.

Note2: VLAN11 is the VLAN towards the edge router and is placed in the VRF

### Switch-1 Ports to IPS placed in EC Bundle:

```
interface GigabitEthernet1/0/10
description To IPS-1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 12,13
switchport mode trunk
channel-group 1 mode on
```

```
interface GigabitEthernet1/0/20
description To IPS-2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 12,13
switchport mode trunk
channel-group 1 mode on
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Centralized IPS Design Using Routing Manipulation

### IPS-1 Interface Configuration:

The screenshot shows the Cisco IOS configuration interface for a switch. The main window displays the configuration for the 'Interfaces' section, specifically the 'Summary' view. The following table represents the data shown in the interface configuration summary:

| Name                  | Mode  | Assigned Default VLAN | Description |
|-----------------------|-------|-----------------------|-------------|
| GigabitEthernet1/0/10 | Trunk | 12,13                 | To IPS-1    |
| GigabitEthernet1/0/20 | Trunk | 12,13                 | To IPS-2    |



For Your Reference

BRKSEC-2002

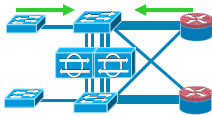
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## IPS High Scalability & Availability Design Considerations

- Don't forget bandwidth!

A design using route manipulation to provide traffic symmetry must consider the traffic capacity of preferred paths



E.g. in the sample design, if one edge router fails, all traffic will be routed over the primary path of the other edge router to the WAN edge distribution.

Consequently, the preferred path must have sufficient bandwidth to accommodate the full traffic capacity.

For high bandwidth design, leverage high speed interfaces, CEF load balancing or ECLB on primary path, etc.

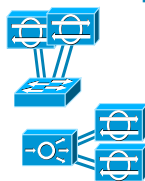
- Understand the load-balancing algorithm of your device

E.g. ECLB on a 3750 is performed based on the characteristics of a flow, not the load, e.g. source and destination address

=> If there is a large amount of traffic on a single flow, all that traffic will be passed to a single IPS

See "Configuring IPS High Bandwidth Using EtherChannel Load Balancing"

[http://www.cisco.com/en/US/products/hw/vpndev/ps4077/products\\_configuration\\_example09186a0080671a8d.shtml](http://www.cisco.com/en/US/products/hw/vpndev/ps4077/products_configuration_example09186a0080671a8d.shtml)



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

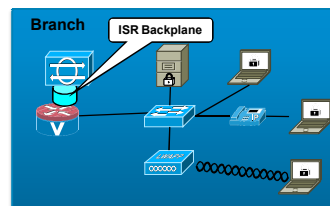
Version 5

## IPS Integration: Sample Distributed IPS Designs

- IPS Module in an ISR

Small, cost-sensitive branch

Consistent, rich IPS signature set

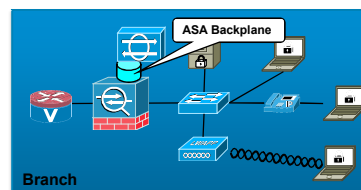


- IPS Module in an ASA

Cost-effective, integrated solution

Consistent, rich IPS signature set

Maintains separate admin domain, e.g. SecOps vs Netops



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

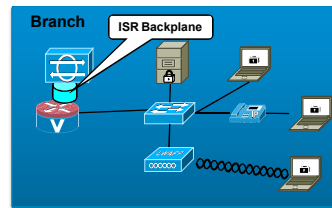
## Sample Distributed IPS Deployment: IPS Module in a Cisco ISR

- Simple integration

Once an IP module is installed in an ISR, enforcement is simply a case of enforcing IPS monitoring on the desired interfaces

Migration from promiscuous to inline mode is a simple configuration change on the interface

```
!  
interface GigabitEthernet0/0.10  
description Wired Data Clients  
encapsulation dot1Q 10  
ip address 10.200.1.1 255.255.255.128  
ids-service-module monitoring inline  
!
```



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

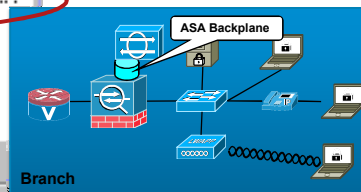
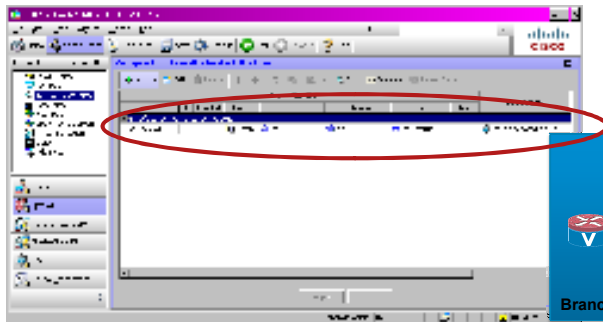
Version 5

## Sample Distributed IPS Deployment: IPS Module in a Cisco ASA

- Simple integration

Once an IP module is installed in an ASA, enforcement is simply a case of enforcing an IPS policy on the desired interfaces

Migration from promiscuous to inline mode is a simple configuration change on the interface



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Cisco IPS: Consistent, rich IPS configuration and policy enforcement across the network...

The image displays a collage of Cisco IPS configuration screenshots and icons for different deployment models:

- IPS Appliance in Internet Edge**: Represented by a blue icon of a server rack.
- IPS Appliance in WAN Edge**: Represented by a blue icon of a server rack.
- IPS Module in ISR**: Represented by a blue icon of a server rack.
- IPS Module in ASA**: Represented by a blue icon of a server rack.

BRKSEC-2002 Version 5

## IPS Integration in the Branch & WAN Edge Design Considerations

- **Monitor wisely**
  - Focus on internal threats, on traffic that truly can be inspected
  - Integrate IPS after VPN termination, firewall, application optimization, etc.
  - => Analysis of authorized, unencrypted, unoptimized traffic
- **IPS scalability and availability**
  - Design according to the scalability of the IPS appliance or the IPS module and host platform model
  - High availability for modules requires a secondary host-device as currently only one IPS module per host-platform
- **Don't forget traffic symmetry**
  - Traffic symmetry is key to the effectiveness of your IPS
  - With one IPS, things are simple but if there are multiple paths, through different IPS, you need to design for symmetrical flows
  - E.g. A branch with multiple edge routers, each with an IPS module

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## IPS Operational Considerations

- **Security Effectiveness: Tune your IPS**
  - Invest the time to tune your IPS – otherwise you'll get so fed up of getting false positives all the time that you'll miss the true anomalies
  - Leverage cross-network correlation – CS-MARS
  - Leverage network & global collaboration
    - Internal IPS sensors, CSA-MC, SensorBase
    - Cisco Live! 2009: ITMATO-2731 - Reputation and Global Threat Data in IPS
- **Facilitate Operations: Common IPS deployment**
  - Use of a common IPS across the entire Enterprise enables tuning to be leveraged across all devices
    - Different platforms/modules but common, consistent configuration and policy enforcement
- **Security Effectiveness: Apply timely signature updates**
  - Signature updates should be updated frequently to ensure maximize threat coverage
    - Schedule outside of typical traffic profile to ensure incidents not missed

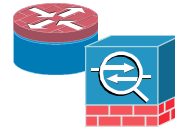
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Detect & Mitigate Malicious Behaviour: Firewall Integration

SAFE Branch and WAN Edge



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Firewall Integration

- Isolate and enforce policy on different security trust domains
  - Trust domains may represent a PoS network, an insecure WLAN handheld network, different user groups, external and internal segments, etc.
- Firewall offers stateful inspection, traffic monitoring, enforcement of network access restrictions and application inspection



### IOS Firewall



- Cost-effective, integrated firewall
- Classic or Zone-Based FW (ZBFW)
  - ZBFW is strategic direction, enabling common policy enforcement across multiple interfaces

### ASA Series



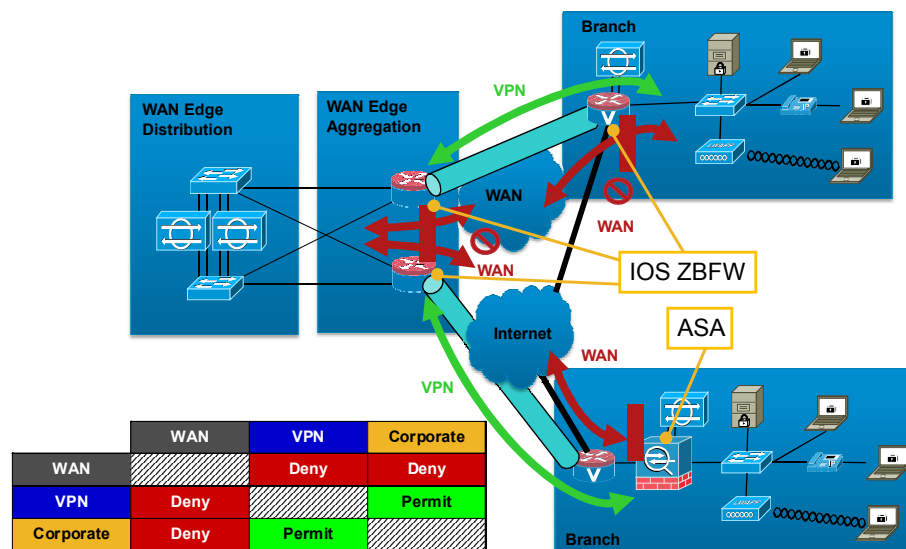
- Highly scalable, high performance, fully featured
- Layer 4 traffic monitoring
- Stateful failover
- Facilitates separate administrative domains (NetOps vs SecOps)

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Firewall Design: Enforcing a Hub-and-Spoke Model



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## Sample ZBFW Design: Enforcing a Simple Hub-and-Spoke Model with Trusted Spokes – WAN Edge Example (1)

### Define Security Zones:

```
zone security VPN  
description VPN to Branches
```

```
zone security Corp  
description Corporate Network
```

### Identify the Spoke Flows:

```
access-list 101 remark Branch Dest  
access-list 101 permit ip any 10.201.0.0 0.0.255.255  
access-list 101 permit ip any 10.200.0.0 0.0.255.255  
access-list 101 deny ip any any
```

```
access-list 102 remark Branch Source  
access-list 102 permit ip 10.201.0.0 0.0.255.255 any  
access-list 102 permit ip 10.200.0.0 0.0.255.255 any  
access-list 102 deny ip any any
```

### Classify the Spoke Flows:

```
class-map type inspect match-any to-branch  
match access-group 101
```

```
class-map type inspect match-any frm-branch  
match access-group 102
```

### Define the Hub-Spoke Policy:

```
policy-map type inspect hub-spoke-policy  
class type inspect to-branch  
pass  
class class-default  
drop log
```

```
policy-map type inspect spoke-hub-policy  
class type inspect frm-branch  
pass  
class class-default  
drop log
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample ZBFW Design: Enforcing a Simple Hub-and-Spoke Model with Trusted Spokes – WAN Edge Example (2)

### Enable flows between the zones and enforce the policy:

```
zone-pair security hub-spoke source Corp  
destination VPN  
service-policy type inspect hub-spoke-policy
```

```
zone-pair security spoke-hub source VPN  
destination Corp  
service-policy type inspect spoke-hub-policy
```

### Place the VPN Tunnel in the VPN Zone:

```
interface Tunnel0  
description VPN to Branches  
zone-member security VPN
```

### Place the Internal Links in the Corp Zone:

```
interface GigabitEthernet0/0/0  
description To switch-1  
zone-member security Corp
```

```
interface GigabitEthernet0/0/1  
description To switch-2  
zone-member security Corp
```

Note1: Since there is an implicit deny once ZBFW is configured, it is not necessary to define and enforce a WAN zone since this traffic is, by default, denied.

Note2: Bi-directional flows must be defined when the policy is to "pass" traffic. If traffic is being inspected, policy is enforced bi-directionally.



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## ASA Design Considerations



- Network access policies enforced based on the security level of an interface

By default, an implicit permit is enforced for interfaces of the same security level, and an implicit permit from a higher to a lower security level interface.

It is recommended to explicitly define policies to be enforced.

- ASA network access policies may also include:

Access edge iACLs for the branch (part of NFP)

WAN edge ACLs, if the branch is hosting externally-accessible services or the branch edge router is not owned and managed by the enterprise.

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## IOS ZBFW Design Considerations



- An implicit deny applies as soon as a single zone is created on a device

Even if an interface is not placed in a zone, traffic will, by default, be denied.

- Policies are, by default, only applied to traffic flowing through the device, not to traffic directed to the device itself

This behavior can be modified by defining policies for what is referred to as the "self" zone.

- Once zones are defined, policies can be tuned and extended according to your deployment needs

Particular traffic and application flows, acceptable use policies

Application inspection – HTTP, SMTP/ESMTP, IMAP, POP, IM

- Stateful inspection requires symmetrical flows

Design for symmetry

For more information, see BRKSEC-2007 – Deploying IOS Security

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Threat Focus Area #3: Attacks Against the Infrastructure

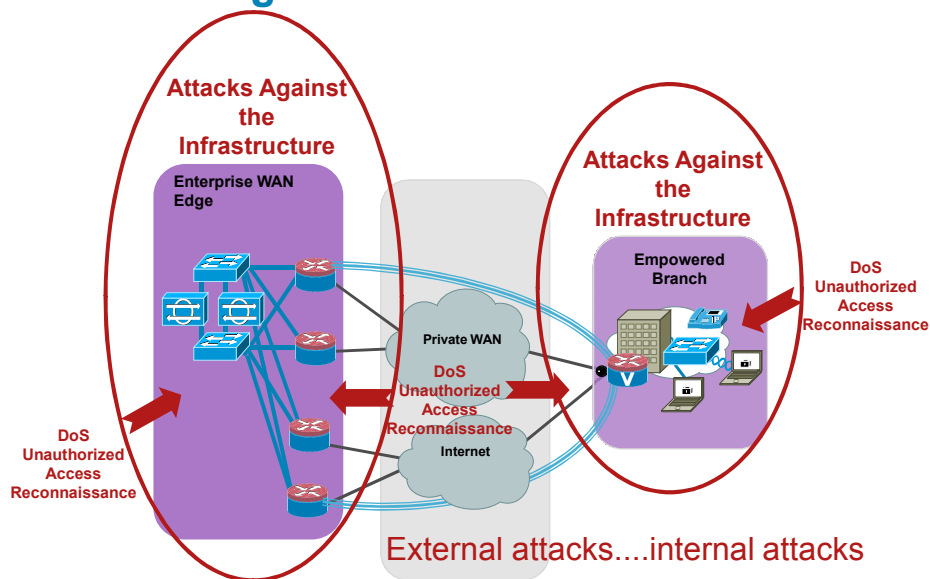
## SAFE Branch and WAN Edge

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Attacks Against the Infrastructure



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

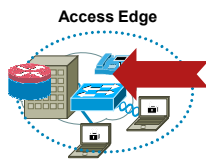
## Infrastructure Attacks on Branch and WAN Edge



- From the outside...

Targeting the branch or WAN edge

DoS attacks, IKE flooding, routing attacks, IP spoofing, unauthorized device access, reconnaissance



- From the inside...

Targeted or indirectly impacting the access edge

Traffic flooding, DHCP starvation, STP manipulation, rogue DHCP server, IP spoofing, ARP spoofing, MiTM attacks, unauthorized device access, scanning, theft of information, reconnaissance, CAM flooding, VLAN hopping, self-DoS

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Protecting the Infrastructure...

- Network Foundation Protection

Lots of stuff to do, much of it not very exciting or cool BUT...

**Absolutely critical to network security**

- Focus is on securing the control and management planes

The network infrastructure is the foundation of the network and **MUST** be secured accordingly

If the infrastructure devices & services are vulnerable, any other additional security layers are futile



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Network Foundation Protection

- Network Foundation Protection Elements

- Secure Routing
- Device & Service Resiliency
- Network Policy Enforcement
- Switching Security
- Secure Device Access
- Telemetry

- Network Foundation Protection Principles

- Restrict attack and vulnerability exposure
- Harden the device
- Harden all services
- Have a backup plan!



...every device, every service

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Branch & WAN Edge: Secure Routing

- Focus on separation of external vs internal routing domains

|                                      |                                                                                                                                             | WAN Edge                                                                                                                                                                                                                                                                       | Branch                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Security Focus               | Routing Security Objectives                                                                                                                 | Implementation on WAN Edge                                                                                                                                                                                                                                                     | Implementation in Branch                                                                                                                                                                                                                                                                                                                                                                                                       |
| Restrict Routing Protocol Membership | Restrict routing sessions to trusted peers and validate the origin and integrity of routing updates                                         | <ul style="list-style-type: none"> <li>Routing peer definition</li> <li>Neighbor authentication</li> <li>TTL Security</li> <li>Default passive interface</li> </ul>                                                                                                            | <ul style="list-style-type: none"> <li>Routing peer definition</li> <li>Neighbor authentication</li> <li>TTL Security</li> <li>Default passive interface</li> </ul>                                                                                                                                                                                                                                                            |
| Control Route Propagation            | Ensure only legitimate networks are advertised and propagated                                                                               | <ul style="list-style-type: none"> <li>Route redistribution filtering to only advertise VPN hub IP address to external routing domain</li> <li>Peer prefix filtering to only accept routes into internal routing domain for branch subnets received over VPN tunnel</li> </ul> | <ul style="list-style-type: none"> <li>Terminate external routing domain on the WAN edge, e.g. using EIGRP stub routing<sup>1</sup></li> <li>Only advertise required routes to the external routing domain</li> <li>Terminate internal routing domain if dynamic routing not required in branch, e.g. using EIGRP stub routing<sup>1</sup></li> <li>Advertise branch routes over the VPN to internal routing domain</li> </ul> |
| Log Neighbor Changes                 | Detect neighbor status changes that may indicate network connectivity and stability issues, due to an attack or general operations problems | <ul style="list-style-type: none"> <li>Neighbor logging on all routing domains</li> </ul>                                                                                                                                                                                      | <ul style="list-style-type: none"> <li>Neighbor logging on all routing domains</li> </ul>                                                                                                                                                                                                                                                                                                                                      |



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Secure Routing Site-to-Site VPN: Internal Domain

### WAN Edge VPN Hub

```
router eigrp 1
network 10.56.0.0 0.0.255.255
network 10.0.0.0
no auto-summary
distribute-list 30 in Tunnel0
passive-interface default
no passive-interface GigabitEthernet1/0/0
no passive-interface GigabitEthernet1/0/1
no passive-interface Tunnel0
!
access-list 30 remark Branch EIGRP Routes
access-list 30 permit 10.200.0.0 0.0.255.255
access-list 30 permit 10.201.0.0 0.0.255.255
<snip>
!
key chain EIGRP-AUTH
key 10
key-string <strong-key>
```

```
interface Tunnel0
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 eigrp-auth

interface GigabitEthernet1/0/0
description To switch-1
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-AUTH
!
interface GigabitEthernet1/0/1
description To switch-2
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-AUTH
!
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Secure Routing Site-to-Site VPN: Internal Domain

### Branch Edge Router

```
router eigrp 1
passive-interface default
no passive-interface Tunnel0
no passive-interface Tunnel1
network 10.0.0.0
no auto-summary
eigrp stub connected summary
!
key chain EIGRP-AUTH
key 10
key-string <strong-key>
!
```

```
interface Tunnel0
description Private WAN Tunnel
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-AUTH
ip summary-address eigrp 1 10.201.1.0
255.255.255.0 5
ip summary-address eigrp 1 10.200.1.0
255.255.255.0 5
!
interface Tunnel1
description Internet Tunnel
ip authentication mode eigrp 1 md5
ip authentication key-chain eigrp 1 EIGRP-AUTH
ip summary-address eigrp 1 10.201.1.0
255.255.255.0 5
ip summary-address eigrp 1 10.200.1.0
255.255.255.0 5
!
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Secure Routing Site-to-Site VPN: External Domain

### WAN Edge VPN Hub

```

router bgp 30000
no synchronization
bgp router-id 192.168.33.3
bgp log-neighbor-changes
network 192.168.0.0 mask 255.255.0.0
redistribute connected route-map VPN-HUB-IP-ONLY
! Define and authenticate peers. Enable BTSH.
neighbor 192.168.33.1 remote-as 65000
neighbor 192.168.33.1 password <strong-password>
neighbor 192.168.33.1 ttl-security hops 2
no auto-summary
!
ip prefix-list VPN-HUB-IP seq 5 permit 192.168.34.1/32
!
route-map VPN-HUB-IP-ONLY permit 10
match ip address prefix-list VPN-HUB-IP
!
    
```

### Branch Edge Router

```

router eigrp 100
passive-interface default
no passive-interface GigabitEthernet0/0
no passive-interface GigabitEthernet0/1
network 192.168.0.0 0.0.255.255
no auto-summary
eigrp stub receive-only
!
    
```

Note: Neighbor logging is enabled by default with EIGRP and thus does not appear in the config.



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Branch & WAN Edge: Service Resiliency

| Service Focus                              | Resiliency | Service Resiliency Objectives                                                                                                                                       | Implementation                                                                                                                                                                                                      |
|--------------------------------------------|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrict attack surface                    |            | Disable unnecessary services<br>Address known vulnerabilities                                                                                                       | <ul style="list-style-type: none"> <li>Disable unnecessary services on all infrastructure devices</li> <li>Patch infrastructure devices with updated software</li> </ul>                                            |
| Harden the device                          |            | Protect device resources from exhaustion attacks by limiting, filtering and rate-limiting traffic destined to the control plane.                                    | <ul style="list-style-type: none"> <li>Limit and rate-limit control plane traffic, including service-specific considerations, e.g. IKE CAC, DAI, DHCP snooping, logging, etc.</li> <li>CoPP if available</li> </ul> |
| Preserve and optimize remote site services |            | Ensure any limited resources at a remote site, such as a low bandwidth WAN link or a low performance platform, are not overwhelmed, and optimize their utilization. | <ul style="list-style-type: none"> <li>End-to-end QoS</li> <li>Application optimization</li> </ul>                                                                                                                  |
| Implement redundancy                       |            | Deploy device, link and geographical diversity to eliminate single points of failure.                                                                               | <ul style="list-style-type: none"> <li>Redundant devices</li> <li>Redundant links</li> <li>Redundant WAN providers</li> <li>Geographically diverse locations</li> </ul>                                             |



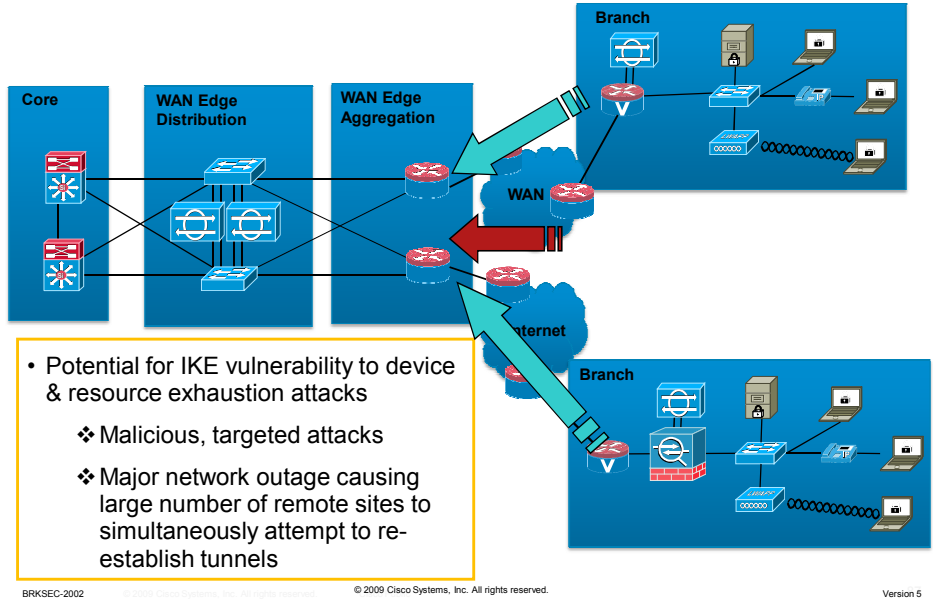
For Your Reference

BRKSEC-2002

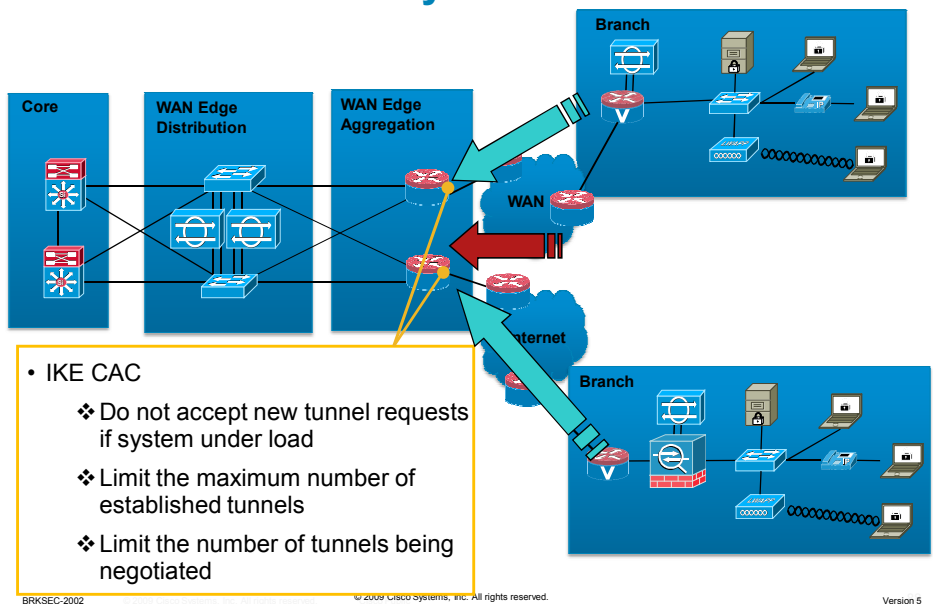
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Service Vulnerability: IKE on VPN Hub



## Service Resiliency: IKE CAC on VPN Hub





## Sample IKE CAC on ASR as VPN Hub

### WAN Edge VPN Hub

```
!  
! Do not accept new IKE SA requests when the  
system resources in use reach this limit  
call admission limit 70000  
!  
! Limit the number of dynamic tunnels  
crypto call admission limit ike sa 500  
!  
! Limit the number of dynamic tunnels in-negotiation  
crypto call admission limit ike in-negotiation-sa  
500  
!
```



For Your  
Reference

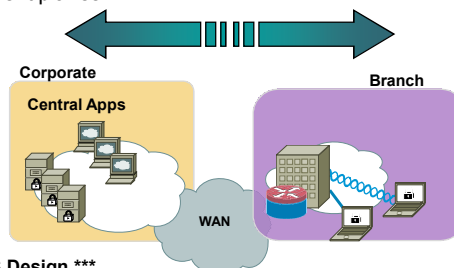
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Service Resiliency: End-to-End QoS

- What does QoS have to do with security?!
  - Ensures service availability, service resiliency, remote manageability
  - Threats include DoS, worms, flooding, overwhelmed router, congested link, etc.
- QoS is critical to successful end-to-end business solutions
  - Protect voice, video and multiple classes of critical data
  - Protect the infrastructure links & devices
  - Protect the control and management planes



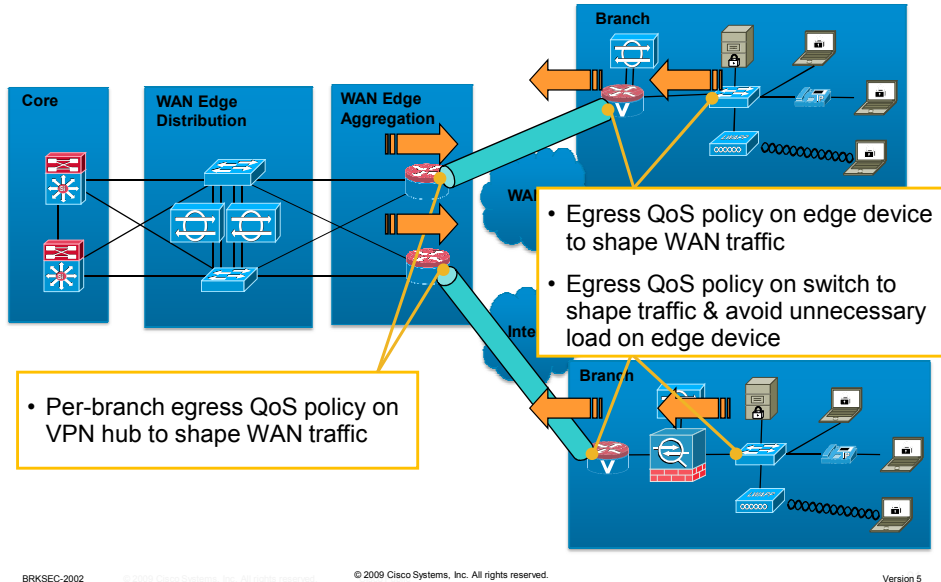
\*\*\* More info: BRKRST-2500: Campus QoS Design \*\*\*

BRKSEC-2002

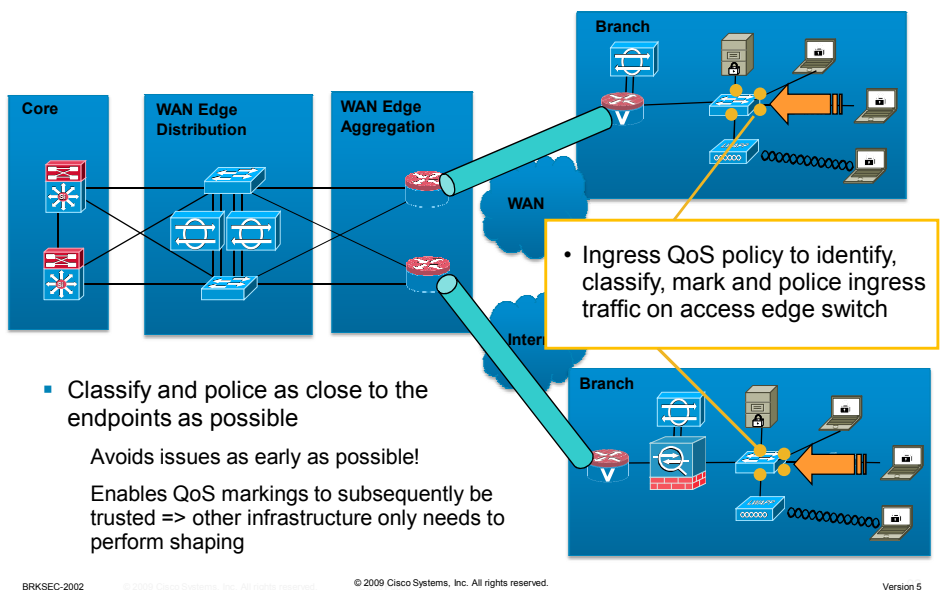
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## QoS: Preserve Branch WAN Link & Branch Edge Device



## QoS: Enforce Consistent Corporate Access Edge Policy



## Sample Per-Branch Egress QoS Policy on ASR VPN Hub: Layer 3 Hierarchical QoS

### 8-class Policy for Rich Media

```

policy-map Child_Branch1
class Voice
  priority percent 18
class Interactive-Video
  priority percent 15
class Call-Signaling
  bandwidth percent 5
class Network-Control
  bandwidth percent 5
class Critical-Data
  bandwidth percent 27
  random-detect dscp-based
class Bulk-Data
  bandwidth percent 4
  random-detect dscp-based
class Scavenger
  bandwidth percent 1
class class-default
  bandwidth percent 25
  random-detect
!
```

```

policy-map WAN-Egress-QoS
class Class-Branch1
  shape average 1310000 13100
  service-policy Child_Branch1
<snip>
!
class-map match-all Class-Branch1
  match access-group name ACL-Branch1
!
ip access-list extended ACL-Branch1
  permit ip any 10.200.1.0 0.0.0.255
  permit ip any 10.201.1.0 0.0.0.255
!
interface Tunnel0
  qos pre-classify
!
interface GigabitEthernet0/0/3
  service-policy output WAN-Egress-QoS
!
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Egress QoS Policy on Branch ISR

### 8-class Policy for Rich Media

```

policy-map WAN-Egress-QoS
class Voice
  priority percent 18
class Interactive-Video
  priority percent 15
class Call-Signaling
  bandwidth percent 5
class Network-Control
  bandwidth percent 5
class Critical-Data
  bandwidth percent 27
  random-detect dscp-based
class Bulk-Data
  bandwidth percent 4
  random-detect dscp-based
class Scavenger
  bandwidth percent 1
class class-default
  bandwidth percent 25
  random-detect
!
```

```

class-map match-all Bulk-Data
  match ip dscp af11 af12
class-map match-all Interactive-Video
  match ip dscp af41 af42
class-map match-any Network-Control
  match ip dscp cs6
  match ip dscp cs2
class-map match-all Critical-Data
  match ip dscp af21 af22
class-map match-any Call-Signaling
  match ip dscp cs3
  match ip dscp af31
class-map match-all Voice
  match ip dscp ef
class-map match-all Scavenger
  match ip dscp cs1
!
interface Tunnel0
  qos pre-classify
!
interface GigabitEthernet0/1
  service-policy output WAN-Egress-QoS
!
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

# Branch & WAN Edge: Network Policy Enforcement

| Network Enforcement Focus | Policy Objectives                                                                                                                | Implementation on WAN Edge                                                                          | Implementation on Access Edge                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Filter Incoming Traffic   | Restrict incoming traffic to authorized sources and for authorized services only                                                 | <ul style="list-style-type: none"> <li>• WAN edge ACLs applied inbound on WAN interfaces</li> </ul> | <ul style="list-style-type: none"> <li>• Access edge iACLs applied inbound on the access edge</li> </ul>                   |
| IP Spoofing Protection    | Ensure traffic is topologically valid, i.e. sourced from a valid address that is consistent with the interface it is received on | <ul style="list-style-type: none"> <li>• uRPF loose mode on WAN interfaces</li> </ul>               | <ul style="list-style-type: none"> <li>• IP Source Guard on access ports</li> <li>• uRPF on Layer 3 access edge</li> </ul> |
| Segment Policy Domains    | Firewall and enforce policy across different security domains                                                                    | <ul style="list-style-type: none"> <li>• VLANs, VRFs</li> <li>• Firewall integration</li> </ul>     | <ul style="list-style-type: none"> <li>• VLANs, VRFs</li> <li>• Firewall integration</li> </ul>                            |



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

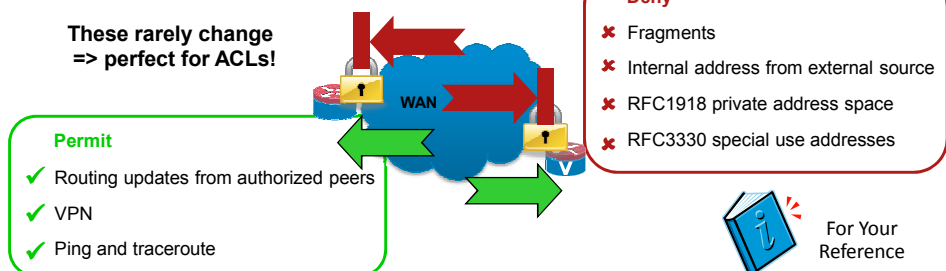
Version 5

## WAN Edge ACLs



- Key objectives of WAN edge ACLs are:
  - Restrict ingress traffic to minimum required traffic and services from authorized originators only
  - Deny traffic with illegitimate, invalid or reserved source addresses
  - Standard ingress edge filtering, per BCP 38 and RFC2827
- For site-to-site VPN, only traffic typically required is:
  - Routing updates from authorized external routing peers only
  - VPN
  - Ping & traceroute for operational purposes

**These rarely change  
=> perfect for ACLs!**



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample WAN Edge ACL: Site-to-Site VPN

### Ingress traffic filtering per BCP 38 and RFC2827

```
access-list 120 remark SP WAN Edge ACL
access-list 120 remark deny Fragments
access-list 120 deny tcp any any log fragments
access-list 120 deny udp any any log fragments
access-list 120 deny icmp any any log fragments
access-list 120 remark deny Incoming with Source=Internal
access-list 120 deny ip 10.0.0.0 0.255.255.255 any
access-list 120 remark deny RFC 3330 Special-Use
Addresses
access-list 120 deny ip host 0.0.0.0 any
access-list 120 deny ip 127.0.0.0 0.255.255.255 any
access-list 120 deny ip 192.0.2.0 0.0.0.255 any
access-list 120 deny ip 224.0.0.0 31.255.255.255 any
access-list 120 remark deny RFC 1918 Reserved Addresses
access-list 120 remark 10.0.0.0/8 and 192.168.0.0/16
omitted as used in testbed
access-list 120 deny ip 172.16.0.0 0.15.255.255 any
```

### Permit routing updates from authorized routing peers only

```
access-list 120 remark permit Incoming BGP from SP
Neighbors
access-list 120 permit tcp host 192.168.33.1 host
192.168.33.3 eq bgp
access-list 120 permit tcp host 192.168.33.1 eq bgp
host 192.168.33.3
access-list 120 permit tcp host 192.168.33.2 host
192.168.33.3 eq bgp
access-list 120 permit tcp host 192.168.33.2 eq bgp
host 192.168.33.3
```

### Permit Site-to-Site VPN

```
access-list 120 remark permit DMVPN with Branches
access-list 120 permit udp any host 192.168.34.1 eq
isakmp
access-list 120 permit esp any host 192.168.34.1
access-list 120 remark permit PKI CA
access-list 120 permit tcp host 192.168.168.226 eq
www host 192.168.33.3
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample WAN Edge ACL: Site-to-Site VPN

### Permit Ping & Traceroute

```
access-list 120 permit icmp any host 192.168.33.3 ttl-
exceeded
access-list 120 permit icmp any host 192.168.33.3 port-
unreachable
access-list 120 permit icmp any host 192.168.33.3 echo-
reply
access-list 120 permit icmp any host 192.168.33.3 echo
access-list 120 permit icmp any host 192.168.34.1 ttl-
exceeded
access-list 120 permit icmp any host 192.168.34.1 port-
unreachable
access-list 120 permit icmp any host 192.168.34.1 echo-
reply
access-list 120 permit icmp any host 192.168.34.1 echo
```

### Enforce Explicit Deny

```
access-list 120 deny ip any any
!
```

### Enforce ACL on WAN Interface

```
interface GigabitEthernet1/0/2
description WAN: Internet
ip address 192.168.33.3 255.255.255.248
ip access-group 120 in
!
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## uRPF on the WAN Edge

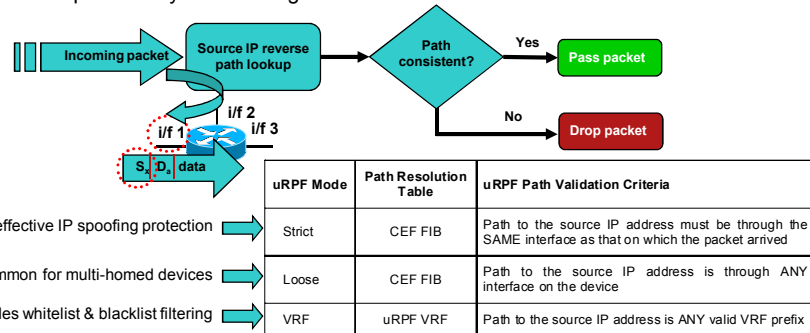


- Unicast reverse path forwarding (uRPF)

Dynamic source IP address validation based on local packet forwarding information

=> Topological validation of source IP addresses

Complementary to WAN edge ACLs



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

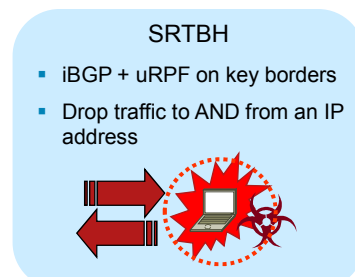
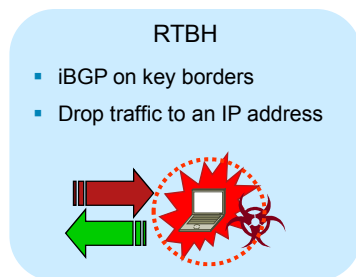
## RTBH/SRTBH: VERY Cool Security Tools (Remote Triggered Black Hole/Source-Based RTBH)

- Highly effective, dynamic and efficient rapid reaction attack tools to mitigate DoS attacks

Single mitigation command

Enforcement in seconds across global networks

Rely on iBGP but you can use BGP just for these brilliant security tools (as well as QPPB) - you don't need to use it for your internal routing



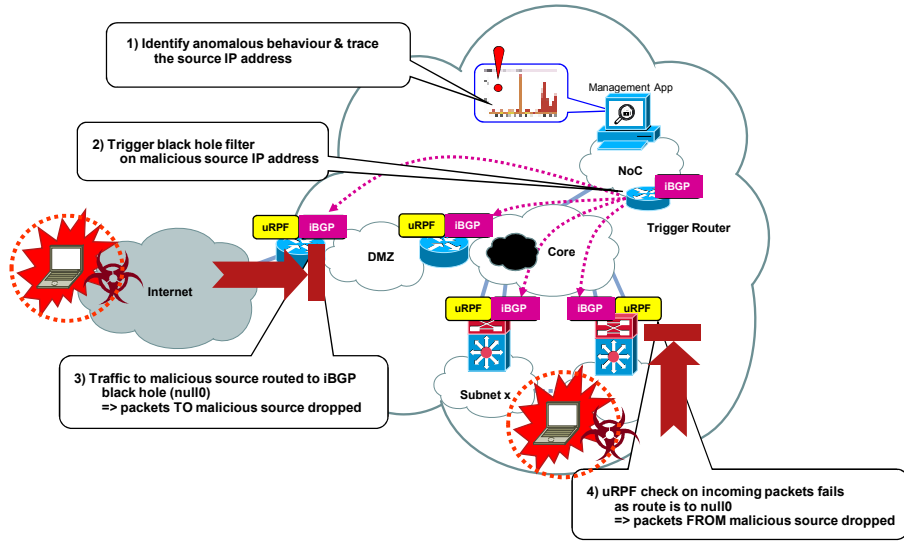
\*\*\* More info: BRKSEC-2204: What can enterprise learn as security practice from Service Providers? \*\*\*

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## SRTBH In Action...Malicious Source



## Branch: Access Edge Switching Security

| Switching Security Focus              | Switching Security Objectives                                                                                                    | Implementation                                                                                                                                                                                                                                                                                                      |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrict Broadcast Domains            | Limit the Layer 2 domain in order to minimize the reach and possible extent of an incident                                       | <ul style="list-style-type: none"> <li>Restrict each VLAN to an access switch.<sup>1</sup></li> </ul>                                                                                                                                                                                                               |
| Spanning Tree Protocol (STP) Security | Restrict STP participation to authorized ports only                                                                              | <ul style="list-style-type: none"> <li>Rapid Per-VLAN Spanning Tree (PVST)</li> <li>BPDU Guard</li> <li>STP Root Guard</li> </ul>                                                                                                                                                                                   |
| DHCP Protection                       | Prevent rogue DHCP server and DHCP starvation attacks                                                                            | <ul style="list-style-type: none"> <li>DHCP Snooping on access VLANs</li> </ul>                                                                                                                                                                                                                                     |
| ARP Spoofing Protection               | Prevent ARP spoofing-based MiTM attacks                                                                                          | <ul style="list-style-type: none"> <li>Dynamic ARP Inspection (DAI) on access VLANs<sup>2</sup></li> </ul>                                                                                                                                                                                                          |
| IP Spoofing Protection                | Ensure traffic is topologically valid, i.e. sourced from a valid address that is consistent with the interface it is received on | <ul style="list-style-type: none"> <li>IP Source Guard on access ports or/ uRPF on Layer 3 access edge or/ ACLs</li> </ul>                                                                                                                                                                                          |
| MAC Flooding Protection               | Prevent switch resource exhaustion attacks that can cause flooding of a Layer 2 domain                                           | <ul style="list-style-type: none"> <li>Port security on access ports</li> </ul>                                                                                                                                                                                                                                     |
| VLAN Best Common Practices            | Apply VLAN security guidelines across the infrastructure                                                                         | <ul style="list-style-type: none"> <li>Define a port as a trunk, access or voice port rather than enabling negotiation</li> <li>VTP transparent mode</li> <li>Disable unused ports and place in an unused VLAN</li> <li>Use all tagged mode for the native VLAN on trunks</li> <li>Traffic storm control</li> </ul> |

\*\*\* Leverage Smartports macros \*\*\*



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## DHCP Protection

- DHCP is brilliant for MiTM attacks and to DoS local users:
  - Rogue DHCP Server
    - Spoof or accidentally bring up a DHCP server
  - DHCP Starvation
    - Exhaust the entire DHCP address space by using a sophisticated DHCP starvation attack
- Cisco IOS DHCP snooping feature addresses both these attack vectors:
  - Rogue DHCP Server Protection
    - If reserved DHCP server responses (DHCPOFFER, DHCPACK, and DHCPNAK) are received on an untrusted port, the interface is shut down.
  - DHCP Starvation Protection
    - Validates that the source MAC address in the DHCP payload on an untrusted interface matches the source MAC address registered on that interface.
- Don't create the potential for a self-DoS!
  - Rate-limit DHCP snooping to harden the switch against a resource exhaustion based DoS attack



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## ARP Spoofing Protection

- ARP spoofing is brilliant for MiTM attacks
  - Send a gratuitous ARP indicating that my MAC address is that associated with the IP address of the default gateway
  - => All traffic flows to me ☺
- Cisco IOS Dynamic ARP Inspection (DAI) feature addresses this attack vector
  - Validates that the source MAC and IP address in an ARP packet received on an untrusted interface matches the source MAC and IP address registered on that interface
  - Basically, it checks that you are who you say you are
- Don't create the potential for a self-DoS!
  - Rate-limit DAI to harden the switch against a resource exhaustion based DoS attack



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5



## IP Spoofing Protection

- IP spoofing is brilliant for all sorts of games:
  - Anonymously launch an attack
  - Spoof the real target - getting others to take out the target
  - Impersonate trusted IP addresses
  - Bypass network security controls completely
  - Snoop data through MiTM attacks
- You have the choice of a few IP spoofing protection techniques:
  - IP Source Guard
    - Ensures that the IP address matches that assigned by DHCP on that interface and on that VLAN
    - Highly effective at mitigating IP spoofing, even within the valid, local subnet range (e.g. right subnet but faked address to bypass access control)
  - uRPF
    - Dynamic Layer 3 IP spoofing protection, validating that the source IP address is topologically valid (=yeah, that IP kinda makes sense here)
  - ACLs
    - Static Layer 3 IP spoofing protection



For Your Reference

**Pick one & deploy it...please!** 😊

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Switching Security Design Considerations



- Make sure you don't create the potential for a self-DoS!
  - Rate-limit switching services and features, including DHCP snooping and DAI
  - Validate impact of features, e.g. port security violation action



- Enforce IP spoofing protection - PLEASE!
  - People should NOT be using invalid, non-topologically correct addresses
  - If they are, they're probably up to no good – so block them!
  - Facilitates so much of security policy enforcement, traceback, etc.



- Operational considerations
  - Leverage "errdisable recovery cause" for automatic recovery
    - Otherwise, port remains in error-disabled state after a security violation => manually recovery required (shut/no shut)
    - BUT be sure to log for visibility

Leverage Smartports macros

Very cool feature enabling customized port templates to be defined according to corporate policy and applied to ports on an as-needed basis

Ensures consistent policy enforcement, eases operations and avoids misconfiguration



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Access Port Macros on 3750

### Unused Ports

```
macro name Unused-Port
switchport access vlan 2000
shutdown
no cdp enable
@
!
```

### Client Access Ports

```
macro name Access-Port
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security maximum 3
switchport port-security maximum 2 vlan access
switchport port-security maximum 1 vlan voice
switchport port-security
switchport port-security aging time 2
switchport port-security violation restrict
switchport port-security aging type inactivity
switchport port-security mac-address sticky
ip arp inspection limit rate 100
load-interval 60
duplex full
priority-queue out
no snmp trap link-status
```

```
storm-control broadcast level pps 1k
storm-control multicast level pps 2k
storm-control action trap
spanning-tree portfast
spanning-tree bpduguard enable
spanning-tree guard root
service-policy input Client-Edge-QoS
ip verify source
ip dhcp snooping limit rate 15
@
!
```

### Applying a Macro

```
switch-1 (config)# default int g1/0/6
switch-1 (config)# int g1/0/6
switch-1 (config-if)# macro apply Unused-Port
switch-1# sh run int g1/0/6
!
interface GigabitEthernet1/0/6
switchport access vlan 2000
shutdown
macro description Unused-Port
no cdp enable
end
```



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## All Infrastructure: Secure Device Access

| Secure Device Access Focus         | Secure Device Access Objectives                                                                                                                                                                                               | Implementation                                                                                                                                                                                                                           |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Restrict Device Accessibility      | Limit the accessible ports and access services, restrict authorized access to authorized services from authorized originators only, enforce session management and restrict login vulnerability to dictionary and DoS attacks | <ul style="list-style-type: none"> <li>Disable ports and services not explicitly required</li> <li>VTY ACLs</li> <li>Reserved last VTY</li> <li>Session timeouts</li> <li>No outgoing access</li> <li>IOS Login Enhancements</li> </ul>  |
| Present Legal Notification         | Display legal notice, developed in conjunction with company legal counsel, for interactive sessions.                                                                                                                          | <ul style="list-style-type: none"> <li>Banners</li> </ul>                                                                                                                                                                                |
| Authenticate Access                | Ensure access is only granted to authenticated users, groups, and services.                                                                                                                                                   | <ul style="list-style-type: none"> <li>Remove default accounts</li> <li>AAA to centralized server for ALL access</li> <li>Unique per-user accounts</li> <li>Minimum access privileges</li> <li>Strong password and key policy</li> </ul> |
| Authorize Actions                  | Restrict the actions and views permitted by any particular user, group, or service.                                                                                                                                           | <ul style="list-style-type: none"> <li>Secrets vs passwords</li> <li>Enable and local user accounts</li> <li>SSH, SCP</li> </ul>                                                                                                         |
| Ensure the Confidentiality of Data | Protect locally stored sensitive data from viewing and copying. Consider the vulnerability of data in transit over a communication channel to sniffing, session hijacking and man-in-the-middle (MITM) attacks.               | <ul style="list-style-type: none"> <li>AAA to centralized server for ALL access</li> <li>Command accounting</li> </ul>                                                                                                                   |
| Log and Account for all Access     | Record who accessed the device, what occurred, and when for auditing purposes.                                                                                                                                                | <ul style="list-style-type: none"> <li>AAA to centralized server for ALL access</li> <li>Command accounting</li> </ul>                                                                                                                   |



For Your Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Secure Device Access on ISR (1)

```
!  
service tcp-keepalives-in  
!  
enable secret <strong-secret>  
!  
aaa new-model  
!  
aaa group server tacacs+ Admin-TAC+  
server 10.242.50.94  
!  
aaa authentication login AuthenExec group Admin-TAC+ local-case  
aaa authentication enable default group Admin-TAC+ enable  
aaa authorization console  
aaa authorization exec AuthorExec group Admin-TAC+ if-authenticated  
aaa authorization commands 15 default group Admin-TAC+ if-  
authenticated  
aaa accounting send stop-record authentication failure  
aaa accounting exec default start-stop group Admin-TAC+  
aaa accounting commands 15 default start-stop group Admin-TAC+  
aaa accounting system default start-stop group Admin-TAC+  
!  
aaa session-id common  
!
```

```
!  
login block-for 100 attempts 5 within 50  
login delay 1  
login quiet-mode access-class 10  
login on-failure log  
!  
username sherelle-admin privilege 15 secret <strong-secret>  
!  
ip ssh time-out 60  
ip ssh authentication-retries 2  
!  
ip tacacs source-interface Loopback0  
!  
access-list 10 remark Last Resort Host  
access-list 10 permit 10.242.50.94  
access-list 111 remark SSH Access  
access-list 111 permit tcp 10.242.50.0 0.0.0.255 any eq 22  
access-list 111 deny ip any any log-input  
access-list 112 remark ACL to Reserve Last SSH Port  
access-list 112 permit tcp host 10.242.50.95 any eq 22  
access-list 112 deny ip any any log-input  
!
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample Secure Device Access on ISR (2)

```
!  
banner exec ^C Your EXEC Banner ^C  
banner login ^C Your Login Banner ^C  
banner motd ^C Your MOTD Banner ^C  
!  
line con 0  
session-timeout 10  
exec-timeout 10 0  
password <strong-password>  
authorization exec AuthorExec  
login authentication AuthenExec  
transport preferred none  
transport output none  
line aux 0  
no exec  
line vty 0 3  
session-timeout 10  
access-class 111 in  
exec-timeout 10 0  
password <strong-password>  
authorization exec AuthorExec  
login authentication AuthenExec  
transport preferred none  
transport input ssh  
transport output none  
!
```

```
!  
line vty 4  
session-timeout 10  
access-class 112 in  
exec-timeout 10 0  
password <strong-password>  
authorization exec AuthorExec  
login authentication AuthenExec  
transport preferred none  
transport input ssh  
transport output none  
line vty 5  
no exec  
!  
!
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Visibility Through Telemetry

### SAFE Branch and WAN Edge



BRKSEC-2002

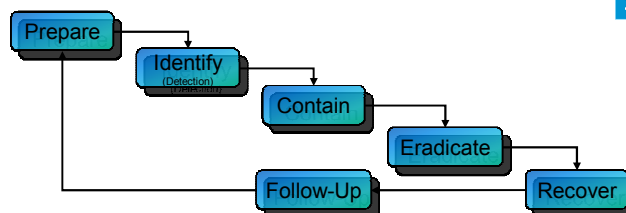
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Visibility is critical to security...



- This is where it all comes together!  
Leverage all your hard work & investment to really increase your security posture
- Effective security is about having the policy, design, deployment, tools, team & operational procedures in place so that...
  - You know **when** bad/odd things are happening
  - You know **what** is happening (what, who, how)
  - You know what to **do** about it



Source: www.sans.org

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

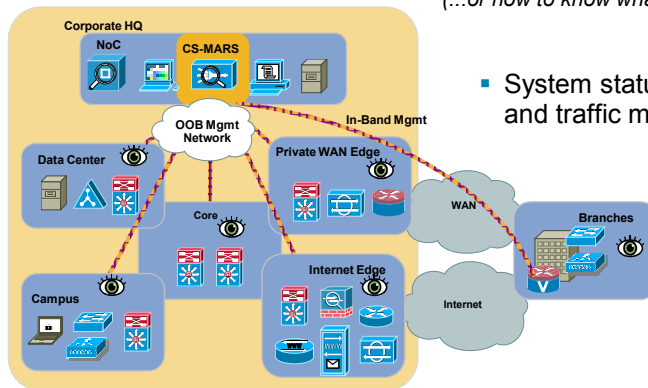
Version 5

## Visibility through Cross-network Telemetry

*Telemetry (noun)*

*the science or process of gathering information about objects which are far away and sending the information somewhere electronically\**

(...or how to know what's going on in your network)



BRKSEC-2002

\*Source: Cambridge Advanced Learner's Dictionary

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Network Telemetry

- Getting started with network telemetry is both inexpensive and relatively simple...

Syslog

SNMP

SDEE

AAA-server based accounting

Netflow

Flow-based traffic monitoring

Who's talking to who, over which ports



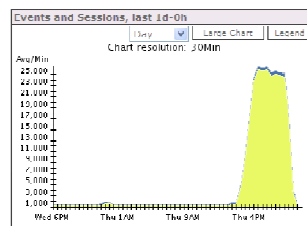
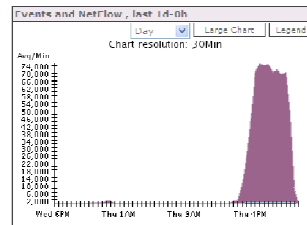
BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Netflow for Traffic Anomaly Detection

- Establishes a network baseline
  - What your traffic profile generally looks like
- Enables investigation into flows
  - Who's talking to who
  - Over which ports
  - To what scale
- Enables traffic anomaly detection
  - Sudden increase in traffic
    - Attack? Outage?
    - New Britney Spears video posted? ;)
  - Anomalous flows
    - Flow from inside to unusual external port
    - Covert protocol channeling? (e.g. BitTorrent over SSH?)



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sampled Netflow on WAN Edge ASR

### Define Sampled Netflow

```
flow-sampler-map NETFLOW-SAMPLED
mode random one-out-of 100
!
```

### Enable Sampled Netflow on WAN & VPN

```
interface Tunnel0
flow-sampler NETFLOW-SAMPLED
ip flow ingress
!
interface GigabitEthernet0/0/3
description WAN: MPLS A
flow-sampler NETFLOW-SAMPLED
ip flow ingress
!
interface GigabitEthernet0/0/4
description WAN: MPLS B
flow-sampler NETFLOW-SAMPLED
ip flow ingress
!
```

```
!
ip flow-export version 5
ip flow-export source GigabitEthernet0
ip flow-export destination <MARS-IP> 2055
!
```



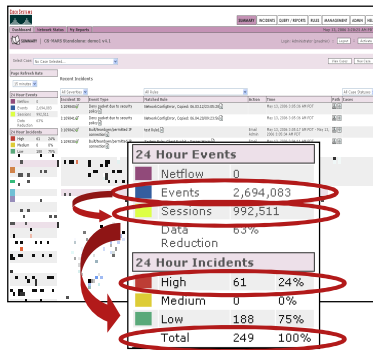
For Your Reference

BRKSEC-2002

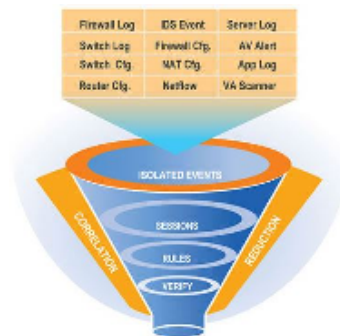
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## CS-MARS for Event Analysis & Correlation



- Ensuring real incidents don't get lost in the noise
- Blended attack detection through cross-network visibility & behavioral analysis



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Telemetry Design Considerations



- Protect the control & management planes
  - Critical to visibility into incidents and ability to react to them
  - => Must be properly isolated, secured and resilient to challenging network events, such as high data rates and worm outbreaks
  - Deploy QoS in hardware, enable device resiliency, CoPP
  - Design well - give your hardware a chance
- Always be aware of the potential for creating a self-DoS!
  - Log wisely
  - Set alerts for CPU & memory thresholds
  - Only log important events
  - Take a look at EEM
  - Use ACL logging only when/where needed
  - Rate-limit logging, reserve memory & limit process statistics
  - No logging console!



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Sample ISR Telemetry Configuration

### • Sync all devices to common timezone & clock

```
ntp authentication-key 10 md5 <strong-key>
ntp authenticate
ntp trusted-key 10
ntp source Loopback0
ntp update-calendar
ntp server 10.56.0.1 key 10
!
```

### • Timestamp events

```
service timestamps debug datetime msec localtime show-
timezone
service timestamps log datetime msec localtime show-
timezone
!
```

### • Syslog to Central Server

```
logging buffered 4096
logging rate-limit all 10
no logging console
logging trap warnings
logging source-interface Loopback0
logging 10.242.50.99
!
```

### • Set Syslog Memory Thresholds Alerts to ~10%

```
memory free low-watermark processor 38721
memory free low-watermark IO 2516
!
```

### • Reserve Memory for Logging

```
memory reserve critical 1000
!
```

### • Enable SNMP & Traps

```
snmp-server community <strong-key> RO 55
snmp-server enable traps envmon
snmp-server enable traps authenticate-fail
snmp-server enable traps cpu threshold
snmp-server host 10.242.50.99 <strong-key> envmon
authenticate-fail memory cpu
!
```

### • Set SNMP CPU Thresholds Alerts & Limit Stats

```
process cpu threshold type total rising 65 interval 5
process cpu statistics limit entry-percentage 40 size
300
!
```



For Your  
Reference

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Threat Mitigation in Action

### SAFE Branch and WAN Edge

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

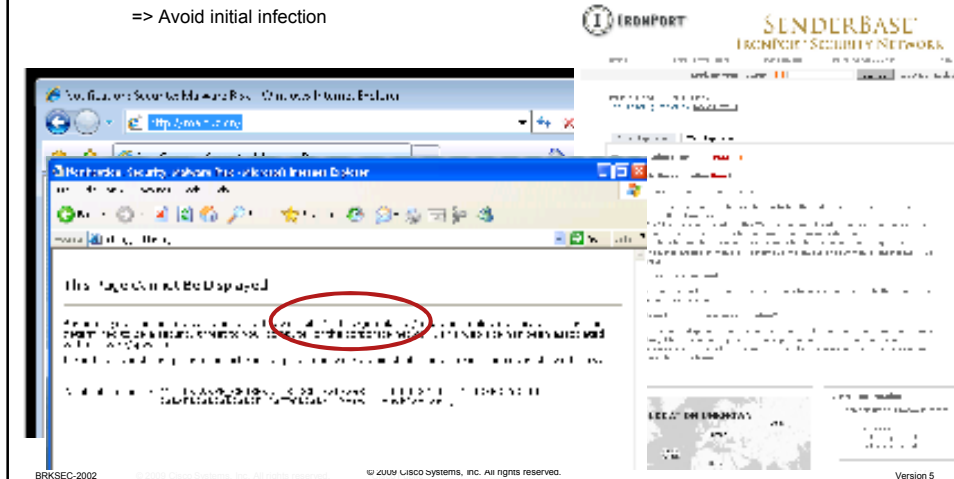


## Branch Client Threat...Gumblar vs WSA

- Client not patched against Adobe PDF or Adobe Flash vulnerabilities & JavaScript enabled but on corporate network, behind Web Security Appliance (WSA)

WSA blocks initial malware download based on domain reputation

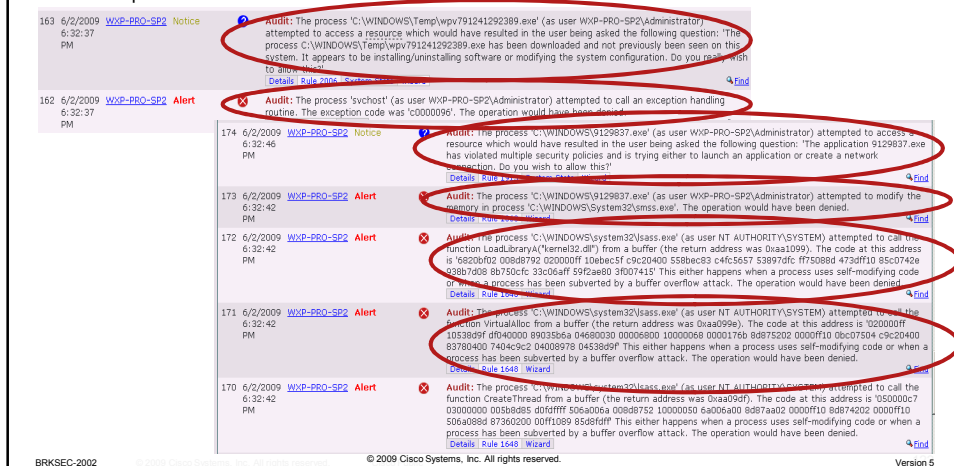
=> Avoid initial infection



## Branch Client Threat...Gumblar vs CSA

- Client not patched against Adobe PDF or Adobe Flash vulnerabilities, JavaScript enabled, not behind WSA, but CSA installed

CSA blocks buffer overflow, system modification, malware installation, etc. with default policies



## Branch Client Threat... Conficker vs CSA

- Client not patched with MS08-67 but CSA installed  
CSA blocks buffer overflow, system modification, etc. with default policies

The screenshot displays a log viewer window with several entries. Two entries are circled in red:

- The top entry is a **Alert** from the process "C:\WINDOWS\System32\cmd.exe" (PID 35) with a severity of "Alert". The message indicates a buffer overflow attempt.
- The middle entry is an **Alert** from the process "C:\WINDOWS\System32\cmd.exe" (PID 35) with a severity of "Alert". The message indicates a system modification attempt.

Other visible log entries include:

- Information**: Administrator login from 192.168.200.141.
- Warning**: Invalid login for administrator admin from 192.168.200.141.
- Notice**: The process "C:\Program Files\adobe\acrobat\acrobat.exe" was user NPL\tech184.

BRKSEC-2002 © 2009 Cisco Systems, Inc. All rights reserved. Version 5

## Branch Client Threat... Conficker vs IPS

- Conficker attempts to propagate on corporate network  
IPS inline blocks initial RPC exploit with default policies & risk rating settings  
Either in branch with distributed IPS or at WAN edge with centralized IPS

The screenshot shows a network diagram on the left and a table of events on the right. Two events are circled in red:

| Event ID | Event Name                    | Severity | Source IP       | Destination IP  | Destination Port | Protocol | Action  |
|----------|-------------------------------|----------|-----------------|-----------------|------------------|----------|---------|
| 1        | Conficker Propagation Attempt | Alert    | 192.168.200.141 | 192.168.200.142 | 135              | RPC      | Blocked |
| 2        | Conficker Propagation Attempt | Alert    | 192.168.200.141 | 192.168.200.143 | 135              | RPC      | Blocked |

BRKSEC-2002 © 2009 Cisco Systems, Inc. All rights reserved. Version 5

## Security for All Services

### SAFE Branch and WAN Edge

BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

## Apply Security Principles to All Infrastructure & Services



- Security policy must be reviewed, updated and enforced according to each network device or service, e.g:

Unified Communications

WLAN



Application Intelligence

Video Services



- Apply the same defense-in-depth approach using the common security framework

Network Foundation Protection

Harden the new network infrastructure devices, update and enforce network policy

Threat control and containment

Extend threat detection and mitigation to the new services

Event monitoring, analysis, and correlation

Ensure visibility into new platforms and services

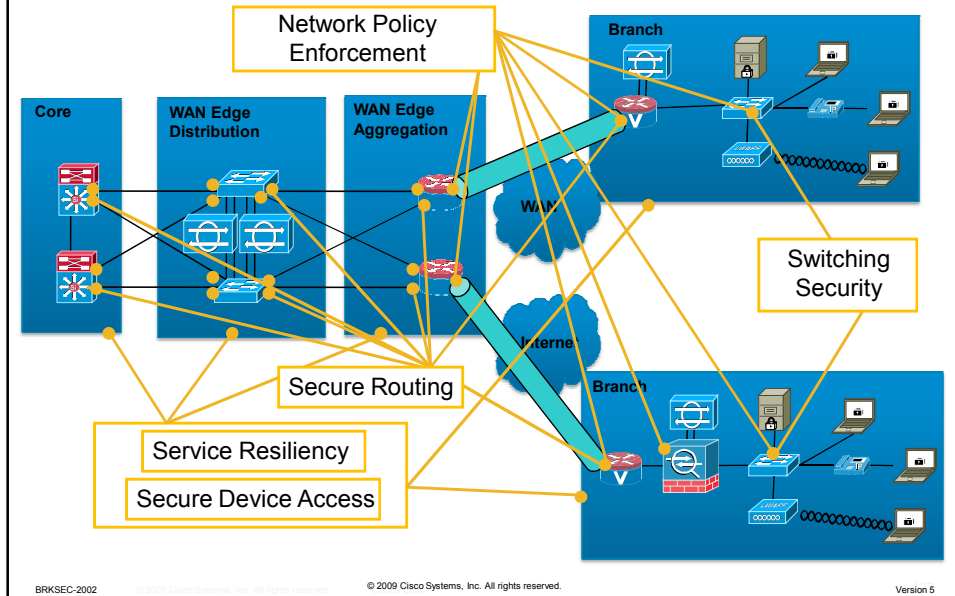


BRKSEC-2002

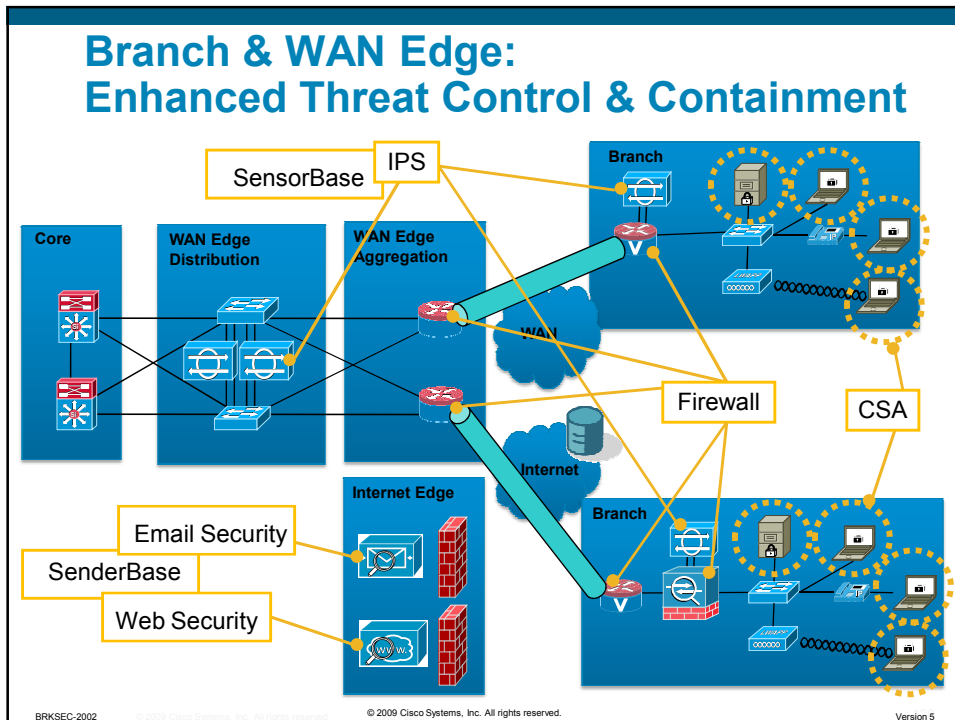
© 2009 Cisco Systems, Inc. All rights reserved.

Version 5

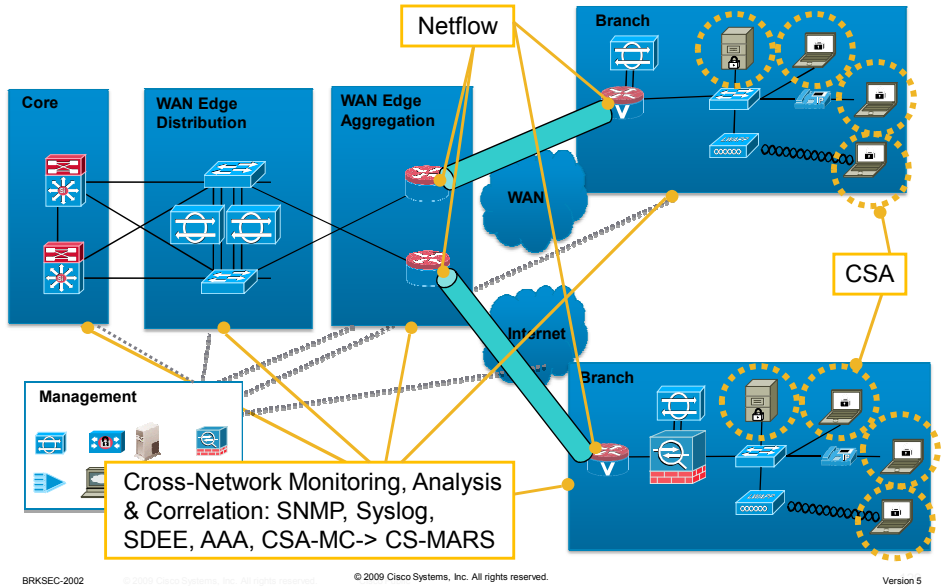
## Branch & WAN Edge: Network Foundation Protection



## Branch & WAN Edge: Enhanced Threat Control & Containment



## Branch & WAN Edge: Visibility



BRKSEC-2002

© 2009 Cisco Systems, Inc. All rights reserved.

Version 5