

# Introduction to Threat Prevention

Module 4: Introduction to Threat Prevention

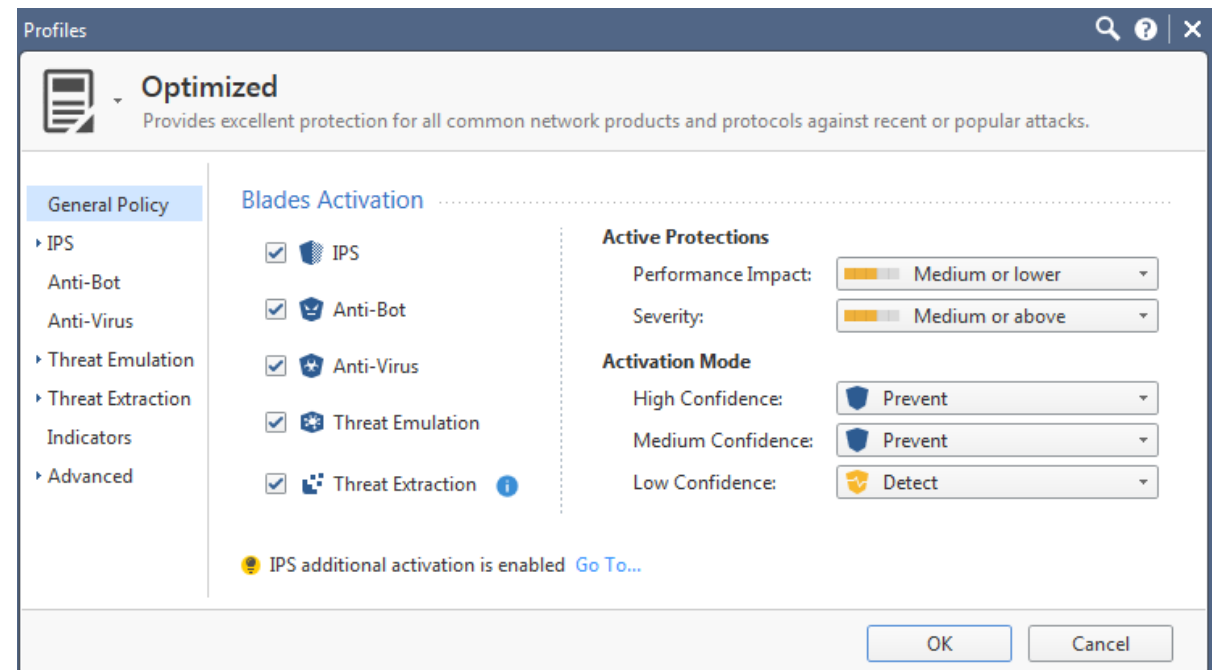
Instructor: Kim Winfield

# Introduction to Threat Prevention Policy

- Create and manage an IPS Policy
- Create and manage an Anti-Virus Policy
- Create and manage an Anti-Bot Policy
- Threat Emulation and Threat Extraction are covered in Module 5

# Create and Manage the IPS policy

- Enabling the IPS Software Blade
- IPS Protections
- Updating IPS Protections



# Enabling IPS Protections

- Client Protections
- Server Protections

Protection	Industry Refere...	Releas...	Update...	Performance Im...	Severity	Confide
Alt-N Technologies SecurityGateway Us...	None	19/06/2008	19/06/2008	<div><div></div></div>	<div><div></div></div>	
Apple QuickTime PICT Image Parsing Ma...	<a href="#">CVE-2007-4672</a> <a href="#">CVE-200...</a>	07/11/2007	07/11/2007	<div><div></div></div>	<div><div></div></div>	
ART Files	<a href="#">CVE-2006-2378</a>	30/06/2006	30/06/2006	<div><div></div></div>	<div><div></div></div>	
Aurigma Multiple ActiveX Kill Bits	None	04/08/2008	04/05/2014	<div><div></div></div>	<div><div></div></div>	
Bad SMTP Server Greeting	None	N/A	N/A	<div><div></div></div>	<div><div></div></div>	
Binary Data In SMTP Commands	None	N/A	N/A	<div><div></div></div>	<div><div></div></div>	
Bind Acks with Invalid Return Ports	None	06/09/2007	06/09/2007	<div><div></div></div>	<div><div></div></div>	
Blaster Attacks	<a href="#">CVE-2003-0352</a>	06/09/2007	06/09/2007	<div><div></div></div>	<div><div></div></div>	
CA BrightStor ARCserve Backup Messag...	<a href="#">CVE-2009-1761</a>	22/07/2009	22/07/2009	<div><div></div></div>	<div><div></div></div>	
CA BrightStor MS-SQL Server ARCserve...	<a href="#">CAN-2005-1272</a>	08/08/2005	11/02/2014	<div><div></div></div>	<div><div></div></div>	
CIFS (SMB) File N				<div><div></div></div>	<div><div></div></div>	
CA BrightStor MS-SQL Server ARCserve Backup Agent Buffer Overflow				<div><div></div></div>	<div><div></div></div>	

Details

Logs

Alt-N Technologies SecurityGateway Username Buffer Overflow

Performance Impact

Low

Severity

High

Attack ID:

[CPAI-2008-085](#)

Last Update:

19-June-2008

Supported Products:

Security Gateway: R77, R76, R75, R71, R70

Threat Description:

The Alt-N Technologies SecurityGateway offers email security with a spam filter that serves as an Exchange or SMTP firewall. A stack-based buffer overflow vulnerability was reported in Alt-N Technologies SecurityGateway. The vulnerability is due to a boundary error in the SecurityGateway that fails to properly handle the username field in certain HTTP requests. An attacker can exploit this issue by sending a specially crafted HTTP request to the target server. Successful exploitation may allow the attacker to execute

Filters

+

Activations

☐ By Profile (298)

Severity

☐ N/A (23)
 ☐ Low (19)
 ☐ Medium (29)
 ☐ High (145)
 ☐ Critical (82)

Confidence Level

☐ N/A (1)
 ☐ Low (36)
 ☐ Medium (181)
 ☐ High (80)

Performance Impact

☐ N/A (1)
 ☐ Very Low (17)
 ☐ Low (140)
 ☐ Medium (101)
 ☐ High (25)
 ☐ Critical (14)































Type

☐ Threat CI (750)

# IPS Protections

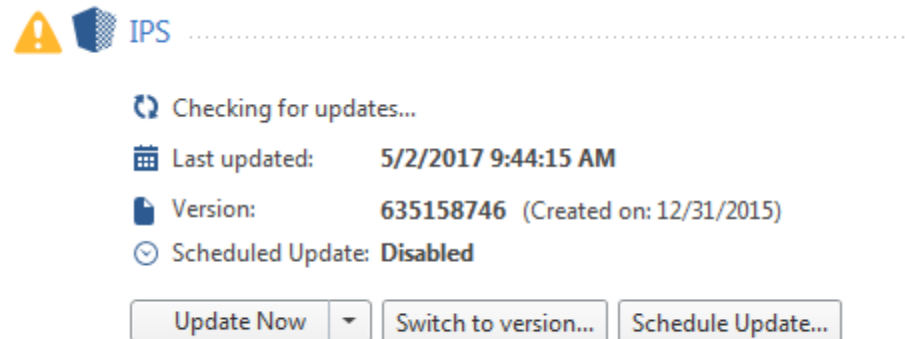
- Browsing IPS Protections
- Activating Protections
- Editing Core IPS Protections

Profiles ⚙️ 👁️ ✎️ 📄 ✕ 📍 🔍 Search...

Name	Active Blades	Performance Impact	Severity	Confidence Level (LowMediumHigh)			Comments
Basic	    	 Medium or lower	 High or above	 Inactive	 Inactive	 Prevent	Provides rel
Optimized	    	 Medium or lower	 Medium or above	 Detect	 Prevent	 Prevent	Provides ex
Strict	    	 High or lower	 Low or above	 Detect	 Prevent	 Prevent	Provide very

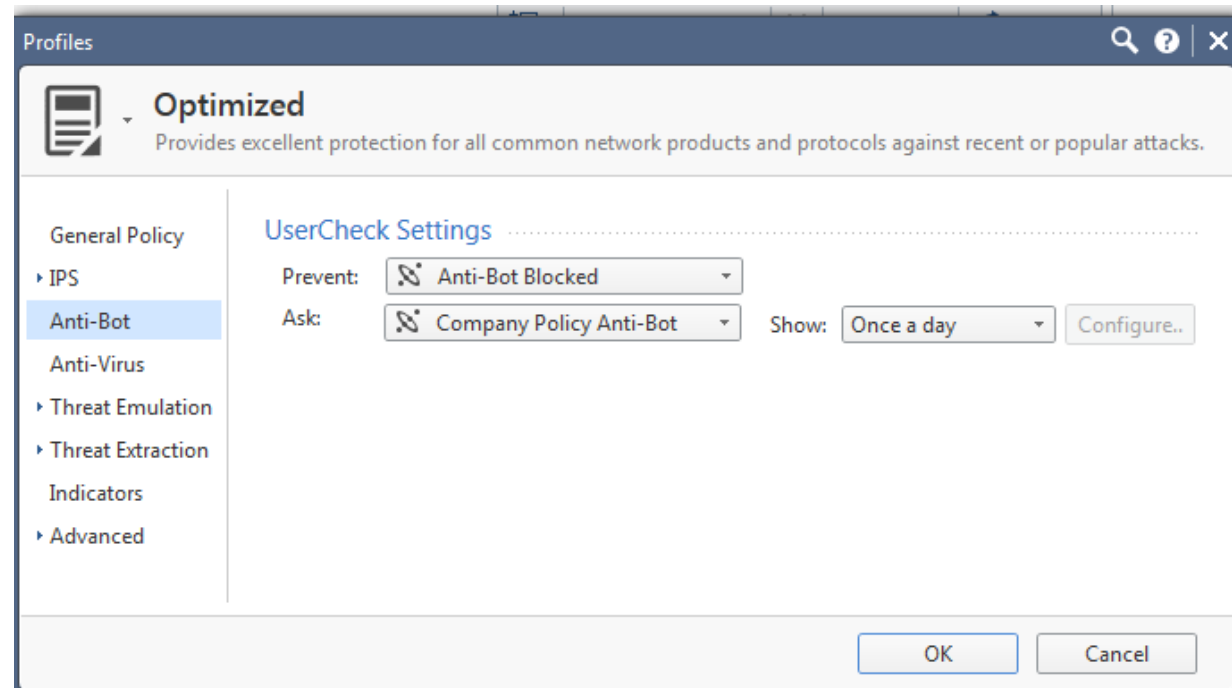
# Updating IPS Protections

- Scheduling Updates
- Reviewing New Protections
- Reverting to an Earlier IPS Protection Package



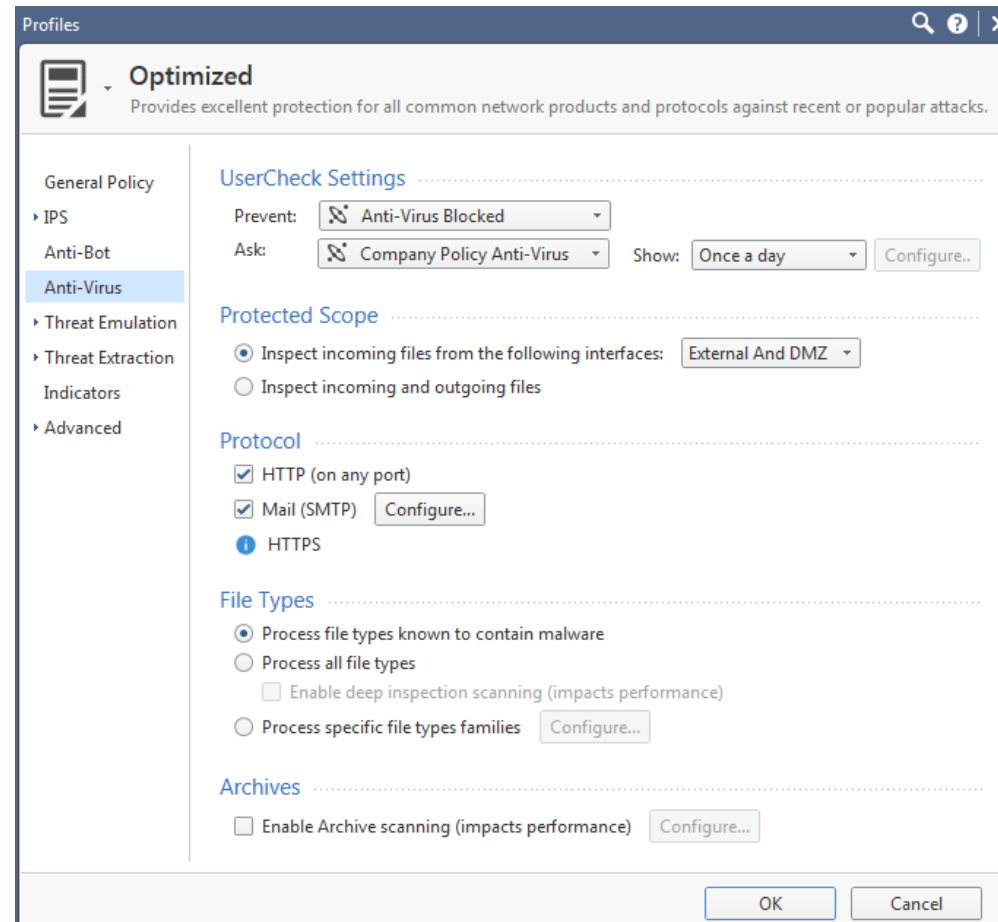
# Configuring Anti-Bot Settings

- Configuring Anti-Bot Settings
- Blocking Bots
- Monitoring Bot Activity



# Configuring Anti-Virus Settings

- Blocking Viruses
- Monitoring Virus Activity





# Summary

- Created and managed an IPS policy
- Created and managed an Anti-Bot policy
- Created and managed an Anti-Virus policy

# Bibliography

*R80.10 Next Generation Security Gateway Getting Started Guide California: USA*

*R80.10 Threat Prevention Administration Guide California: USA*