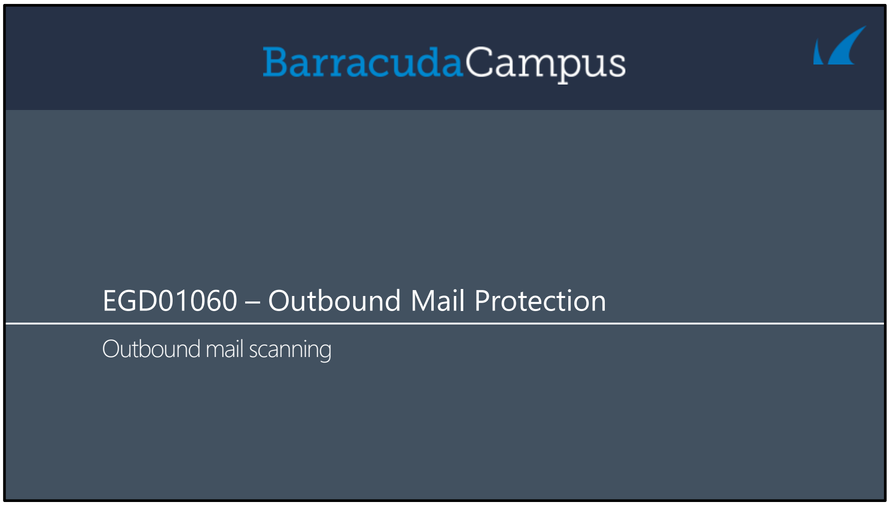
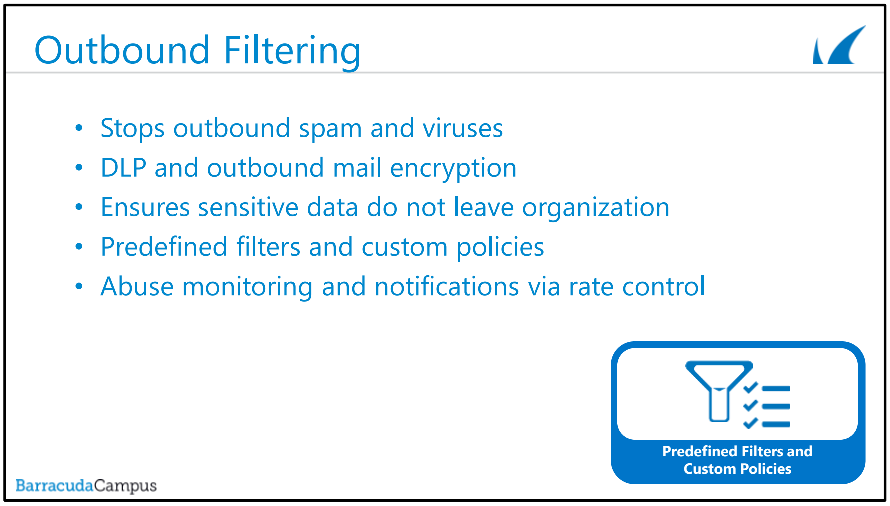


BarracudaCampus

EGD01060 – Outbound Mail Protection

Outbound mail scanning

Training Video Transcript



Outbound Filtering

- Stops outbound spam and viruses
- DLP and outbound mail encryption
- Ensures sensitive data do not leave organization
- Predefined filters and custom policies
- Abuse monitoring and notifications via rate control

Predefined Filters and Custom Policies

BarracudaCampus

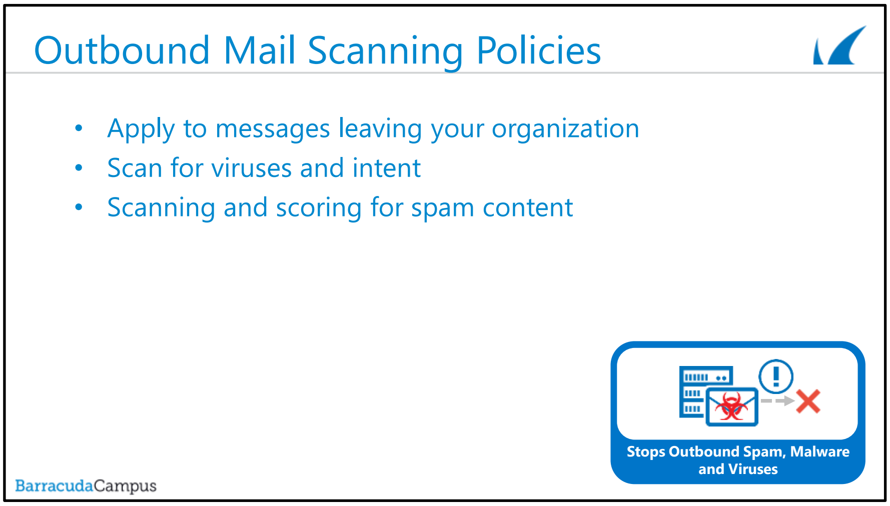
Training Video Transcript

Spam isn’t just a problem with inbound mail, outbound mail is also prone to spam and virus problems. It’s common for some types of malware to send spam and viruses from compromised workstations without a user’s knowledge. This is an issue for many reasons. Among other things, if outside recipients receive a lot of spam from your email server, your organization might find itself on a block list, and then no one will receive any messages you send. Outbound filtering prevents organizations from being put on spam block lists and prevents sensitive data in email from leaving the organization. Employees can inadvertently cause internal systems to become a source for botnet spam. Using a subset of its defense layers, the Email Gateway Defense’s outbound filtering stops outbound spam and viruses.

It also lets administrators enforce content polices for Data Loss Prevention (DLP) and to meet other content standards in outgoing email.

Predefined filters and custom policies can be used to detect sensitive data and block or encrypt email.

Outbound email traffic is automatically monitored for Rate Control by Email Gateway Defense. If the volume of outbound mail messages from the service exceeds normal levels during a 30-minute time frame, the Rate Control feature takes effect and outbound mail is deferred until the end of that time frame.



Outbound Mail Scanning Policies

- Apply to messages leaving your organization
- Scan for viruses and intent
- Scanning and scoring for spam content

Stops Outbound Spam, Malware and Viruses

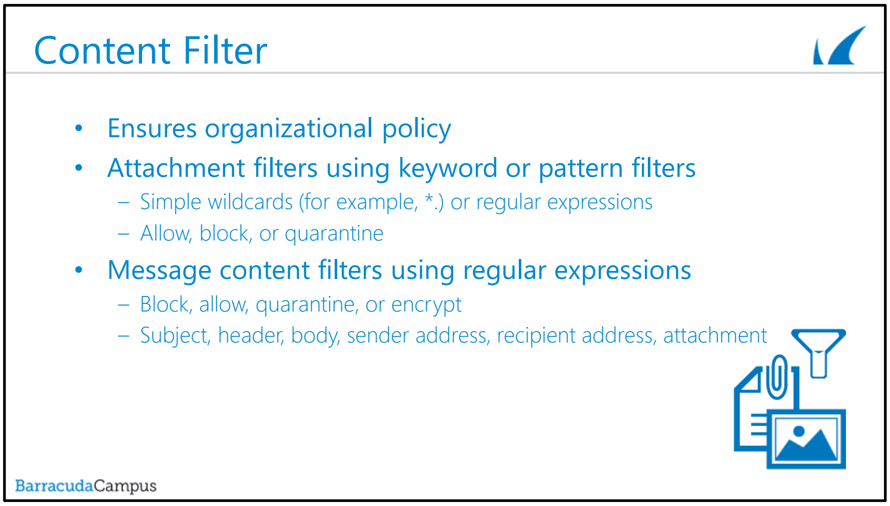
BarracudaCampus

Training Video Transcript

By scanning all outbound messages, you can ensure that all email leaving your organization is legitimate, virus free, and does not leak private or sensitive information from inside the organization.

By default, the Email Gateway Defense scans all outbound mail for virus intent and spam content. If a virus or spam is discovered in an outbound message, the message is not delivered; however, the administrator can manually deliver mail caught for spam. The Email Gateway Defense sets default outbound rate limits; senders and IP addresses cannot be exempted.

Outbound mail scanning includes spam and virus scanning; IP address filtering; sender domain, username or email address filtering, recipient email address filtering, content filtering, attachment filtering, and intent analysis. As with inbound mail, a score is assigned based on the likelihood that the content represents spam content.



Content Filter

- Ensures organizational policy
- Attachment filters using keyword or pattern filters
  - Simple wildcards (for example, *.) or regular expressions
  - Allow, block, or quarantine
- Message content filters using regular expressions
  - Block, allow, quarantine, or encrypt
  - Subject, header, body, sender address, recipient address, attachment

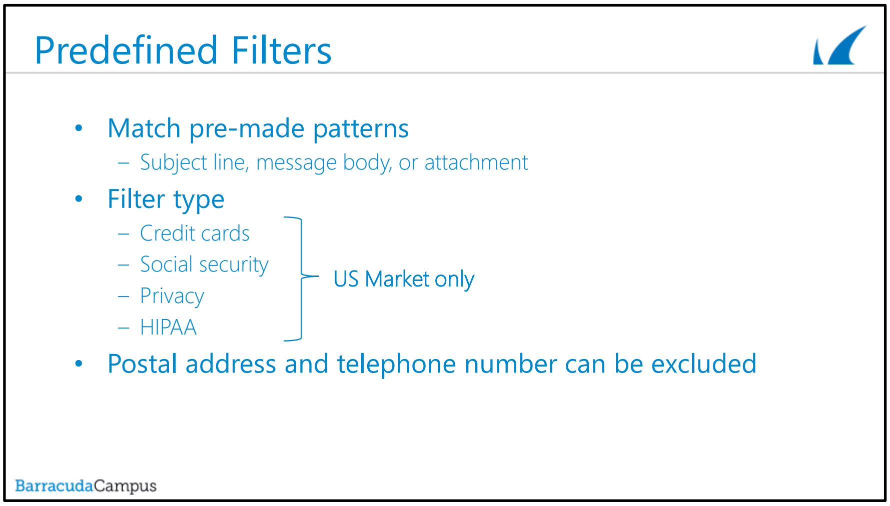
BarracudaCampus

Training Video Transcript

To ensure adherence to organizational policy, content filters can be used. In line with policy, filters can ensure, for example, that emails don't contain details relating to bank accounts, personal information, or that attachments of a particular type aren't passed on externally.

Use attachment filters to block, quarantine, or ignore messages that contain attachments with file name patterns or MIME types. To take an action based on a file name, enter a filename pattern using an asterisk as a wildcard, and then indicate the action to take on the attachment. For example, to block all ZIP files, enter *.zip, and select the Block action. To specify MIME types, enter the MIME type pattern, and select the desired action. For a list of example MIME types, click the Help button on the Outbound Settings - Content Policies page in the web interface. Additionally, you can take actions on attached archive files that require a password to unpack the file.

To control message delivery, customize content filtering based on characteristics of the message's Subject, Header, Body, Sender, Recipient, or Attachments. Specify simple words or phrases when you create filters, then choose where you want to apply those filters for outbound messages. Please note that content filtering is not case sensitive.



Predefined Filters

- Match pre-made patterns
  - Subject line, message body, or attachment
- Filter type
  - Credit cards
  - Social security
  - Privacy
  - HIPAA

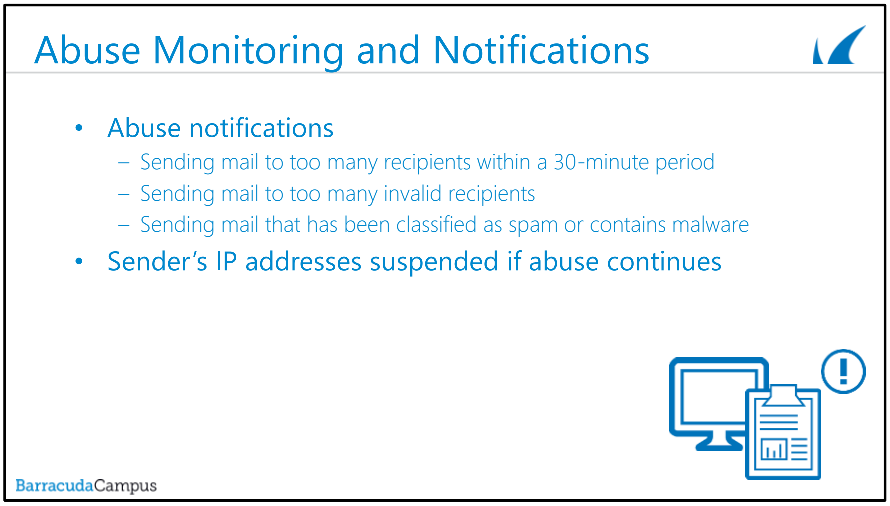
  US Market only
- Postal address and telephone number can be excluded

BarracudaCampus

Training Video Transcript

The Email Gateway Defense also includes predefined filters that allow you to block, quarantine, or encrypt outbound messages based on predefined data leakage patterns (specific to the US), for example, social security numbers detected in the message subject, body, or attachments.

If necessary, you can create exceptions to predefined HIPAA or Privacy content filters to prevent outbound messages that include phone numbers and street addresses from being blocked, encrypted, or quarantined.



Abuse Monitoring and Notifications

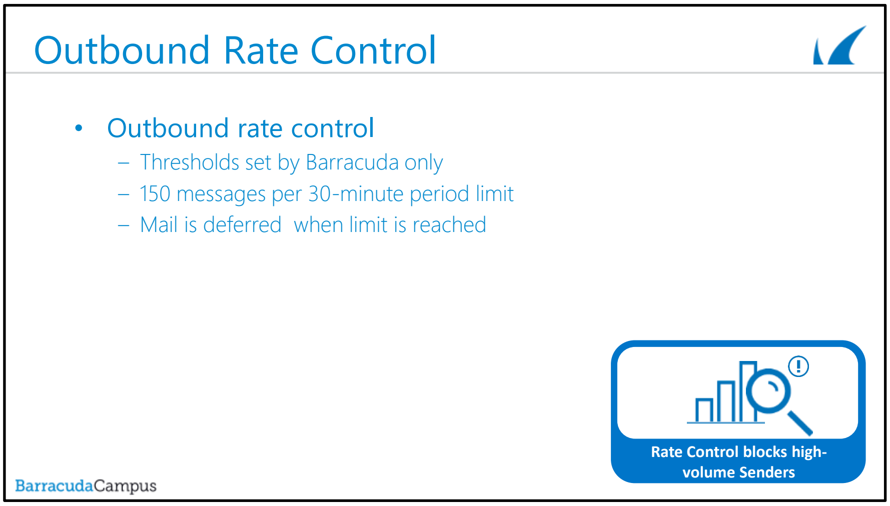
- Abuse notifications
  - Sending mail to too many recipients within a 30-minute period
  - Sending mail to too many invalid recipients
  - Sending mail that has been classified as spam or contains malware
- Sender's IP addresses suspended if abuse continues

BarracudaCampus

Training Video Transcript

The Email Gateway Defense admin receives notifications for various reasons, including sending mail to more than 150 recipients per 30 minute period; sending out mail to more invalid recipients than allowed, or sending out mail classified by the service as spam or as containing a virus.

If your network sends out a large email blast, this may trigger an abuse notice from the Barracuda Email Gateway Defense. This notice informs you that you are sending out mail to more than 150 recipients per 30 minute period. This is not a block of your mail, but it delays delivery of the messages. The mail will eventually go out, but at a much slower rate over a longer period of time.



Outbound Rate Control

- Outbound rate control
  - Thresholds set by Barracuda only
  - 150 messages per 30-minute period limit
  - Mail is deferred when limit is reached

Rate Control blocks high-volume Senders

BarracudaCampus

Training Video Transcript

Outbound rate limits are applied to protect against spam and mass-mailing malware from compromised accounts. It helps prevent spammers and hackers from compromising your email server by relaying mass mailings. Outbound rate control is not an outbound mail block; mail is deferred allowing your mail server to retry the mail until it is delivered.

This rate limit defines the maximum number of messages an individual user on the Email Security account can send out in a 30-minute period. By default, the service outbound rate limit is set to 150 messages per 30 minutes per registered user. This means 7200 messages per day. Exceeding this number results in deferral of the additional mail. If users are hitting this rate limit, then they are sending more than 150 messages in a 30-minute period.

Thank You

BarracudaCampus

Training Video Transcript